COMBATING TERRORISM CENTER
at West Point

Remotely Piloted Innovation

Terrorism, Drones and Supportive Technology

Don Rassler

Remotely Piloted Innovation:
Terrorism, Drones and Supportive Technology

Don Rassler

Combating Terrorism Center at West Point

United States Military Academy

www.ctc.usma.edu

October 2016

Cover Photo: An unmanned drone aircraft is part of a display during a press conference in Peshawar on September 13, 2005. Pakistani forces recovered an unmanned drone aircraft and a major weapons cache in a raid on a suspected al-Qa`ida hideout in the tribal areas near Afghanistan, a top commander said. (TARIQ MAHMOOD/AFP/Getty Images)

CONTACT

Combating Terrorism Center

U.S. Military Academy

607 Cullum Road, Lincoln Hall

West Point, NY 10996

Phone: (845) 938-8495

Web: www.ctc.usma.edu

ACKNOWLEDGMENTS

This project would not have been possible without the input and support provided by several people. The author would like to thank LTC Bryan Price for supporting this effort when it began several years ago, and Muhammad al-`Ubaydi for his research assistance and the key role he played in getting this project started. The great feedback the author received from his CTC colleagues Brian Dodwell, Arie Perliger and Daniel Milton, and from the report's two external reviewers, Paul Scharre and Brian Jackson, was also critical, and helped significantly to improve the final product. CTC intern Brandon Mohr also deserves a thank-you for producing several of this report's graphics.

Don Rassler

TABLE OF CONTENTS

List of Figures

Executive Summary

In mid-August 2016, the Shiite militant group Hezbollah reportedly dropped two small bombs from what is believed to have been a modified, commercially available drone that it was flying over rebel positions in Syria. While terrorist groups have long had a fascination with drones and experimented with their use, the incident was a first for a terror group, and it potentially represents the leading edge of a wave of similar incidents that could follow in the months, years and decades ahead.

Much has been made of the threat of terror use of drones (also known as "uninhabited aircraft systems," or UASs), but little empirical and historical work has been done to support our understanding of this phenomenon and its evolution. This report seeks to address this gap by providing a review of, and framework to situate, cases in which terrorist entities have either shown a substantive interest in drones or have used them. It evaluates both individual use cases and the activity of groups that have used drones frequently enough to constitute their having a "program." These cases are then complemented by a review of the creative ways that private citizens have used drones, in order to provide decisionmakers with a firmer baseline of both demonstrated terror capability and what lies within the immediate realm of possibility, given what has already been achieved by others. This report also includes an overview of new technologies that are likely to further complicate the scope of this developing threat.

Situating Terror UAS Use: A Framework

Drones provide a number of benefits and can be used by terrorist entities in five primary ways: for surveillance; for strategic communications; to smuggle or transport matériel; to disrupt events or complement other activities; and as a weapon. This last category includes instances of a drone being piloted directly to a target, a drone delivering explosives, and a weapon being directly mounted to a drone.

The Threat: General Overview

The cases reviewed in this report reveal that the current threat of a terrorist entity using a single drone navigated via remote control is a moderate probability, and low-to-moderate consequence event in terms of lethality. And while any future terror drone attack using one platform will certainly be novel and noteworthy, and will help a group gain additional publicity, such an attack is unlikely to be strategic in nature—unless a drone is used by a terror entity to successfully carry out a targeted assassination; to kill individuals in or gain significant access to a heavily denied area; or to successfully disperse chemical, biological or radiological weapons. A drone could also be used in such a shock-inducing, well-publicized or creative way that the ingenuity of the attack itself would constitute it being strategic.

The number and sophistication of drones used is also likely to enhance the scope and seriousness of the threat, and to affect the consequence of future incidents. For example, a drone attack involving the use of a small group of drones, or a swarm of drones guided by autonomous features, has the potential to up the ante in terms of an attack's lethality, its psychological impact and its complexity.

Threat Trajectory: Interest, Demonstrated Capability and Specific Findings

Terrorist interest in drones is anything but new. While terror groups' interest in and use of drones has become more frequent over the last decade, especially as commercially available variants of drones have become more popular, sophisticated and accessible, the first documented terror case occurred more than two decades ago, when the Japanese apocalyptic group Aum Shinrikyo considered using a drone to distribute sarin gas.

Use Becoming More Frequent, but Impact Still Limited

While many terror groups or individuals have shown an interest in UAS technology, few have successfully deployed it in any meaningful way. Terrorists' use of drones has certainly complicated some conflicts, but the use of this technology by terrorists has yet to change or significantly alter the direction of any conflict, and so the broader impact of this tool thus far has been quite limited.

Single drones have been used by terror entities primarily for surveillance and strategic communications, and it is in this area where terrorists have made the most gains. Besides Hezbollah, the Islamic State, and Jabhat Fateh al-Sham no other terror groups or terror-linked individual are believed to have successfully used a weaponized UAS to date in an operation. The Islamic State, at the time of writing, appears to be the only group that has used a weaponized drone to kill. HAMAS has also reportedly flown a weaponized drone, but it has yet to succeed in using a UAS in a lethal way as part of an attack. There have also been seven other times when another group or individual possessed a drone and weaponization appears to have been a goal.

Program Concentration vs. Broader Geographic Proliferation of UAS Interest and Use

The four terror groups with identifiable drone programs are all based in the Levant and control some form of territory. Three of these groups also engage in governance and conduct state-like activity. But when individual cases are considered, the list of terror entities that have shown an interest in using drones to support their operations is much more geographically diverse. To date, incidents have occurred in Colombia, Egypt, Germany, Iran, Iraq, Israel, Japan, Lebanon, Pakistan, Palestine, Spain, Syria and the United States.

Group Types and Organizational Dynamics

The types of terror groups that have demonstrated an interest in drones are also ideologically diverse. While the majority of cases are heavily skewed towards those inspired by radical conceptions of Islamic ideology (from both Sunni and Shi`a schools of thought), terrorist use and interest in drones also includes entities motivated by apocalyptic, right-wing and irredentist ideologies. This suggests that future terror use of this technology will not be limited to groups of one type of extremist ideology, but will instead involve many such groups.

Groups with contemporary drone programs are also older and comparatively well experienced. Indeed, the organizational histories of Hezbollah, HAMAS and the Islamic State all stretch back more than a decade. Other groups that showed an early interest in drones, such as Aum Shinrikyo, FARC, Lashkar-e-Taiba and the Haqqani Network, were also those that were relatively more mature and had demonstrated a track record of innovative behavior.

Individual, One-Off Cases Are Mixed—More Inspired and Less Networked

Only one of the thirteen individual cases reviewed for this report has proven ties to al-Qa`ida. Further, the author of this paper was unable to find evidence of any Islamic State–inspired, individual drone plots outside the territory in Syria in Iraq that the group has dubbed "the Caliphate."

Limiting Factors: Technical Features, Specific Choices and Countermeasures

Three factors explain the inability of terrorist entities to successfully weaponize a drone to inflict significant harm: First, the limitations associated with the range, endurance and payload of commercially available drones. Second, the specific choices made by terrorists. And third, the countermeasures that states have developed to defeat hostile drones. These limiting factors do not mean that there is no

room for surprises, or that these challenges and obstacles cannot be overcome.

Extending the "Realm of the Possible": Private Citizens and Additional UAS Capability

Driven by their own creativity and a do-it-yourself ethic, private citizens have also developed a number of unique ways that commercial drones can be used. Some of the more noteworthy innovations include: the modification of a drone to collect electronic intelligence (2011); the firing of a handgun (2008) and a flamethrower (2015) mounted to a drone; and the attachment of an aerosol device to a drone by a graffiti artist (2015). For a terrorist group interested in inflicting harm, these innovations demonstrate additional capability, and they could be repurposed to extend what lies within the immediate realm of the possible. A number of close encounters between drones and airliners, as well as a handful of lethal accidents involving hobbyist drones, illustrate additional threat potential.

Complicating Factors

Future off-the-shelf drones will be able to carry heavier payloads, fly and loiter longer, venture farther from their controller and be able to do so via more-secure communications links. The increased speed of small drones and advancements in sensors and drone add-on technology (such as infrared and night vision cameras), will compound the problems for counterterror organizations. Additional complications will arise from such things as decentralized manufacturing processes facilitated by 3-D printing, which will make field drone production and related repairs easier.

This naturally also means that the tools to counter, disable or defeat drones will become more capable too. The broader use of commercial drones will be accompanied by regulatory changes that will likely lead to a further rationalization of airspace and export control restrictions; these factors could make it harder for terrorist actors to acquire specific technology or to fly drones when and where they like.

Emerging technologies that have disruptive potential complicate things even more. Some of the most significant technologies that will drive changes in drone capabilities include artificial intelligence; autonomous systems and robotics; miniaturization and swarming; nanoexplosives and directed energy weapons; enhanced processing power and data mining; and cyber tools. While each of these technologies will present its own set of counterterrorism challenges, future terror drone threats will likely combine the use of several of these technologies as a system.

Implications

Data Collection: If not already being done on a broad scale, the U.S. government should start systematically cataloging cases of drone use by terrorists, as well as cataloging the innovative ways citizens use drones. Such a database will inform resourcing and regulatory decisions, and promote more effective drone policies.

Multidisciplinary Monitoring: To limit the risk of strategic surprise, analysts following this issue should monitor innovations across a number of spheres; such analysts must be part terror specialist, part technologist, and part industry expert. Analysts should also be schooled in the monitoring and collection of open-source data, as the overwhelming majority of game-changing developments in this arena are taking place in plain sight.

Applicability of Research to Other Related Threats: Terrorists' use of drones is only one dimension of a much broader issue, as remotely controlled and autonomous/smart technologies can also be used on land and at sea. Equal attention, and projected thinking, should be given to evaluating terrorists' innovation in these areas as well, as, for example, emerging technologies like self-driving cars create new opportunities.

Introduction

As noted by Brian Michael Jenkins, most of "today's terrorists want a lot of people watching and a lot of people dead."[1] To accomplish these objectives, and to outbid rivals for the spotlight, entities like the Islamic State seek to use more-lethal methods of attack and to execute people in shock-inducing ways, such as drowning them while locked in a steel cage.[2] For a number of terrorists operating in today's media-saturated environment, novelty is sought out as a form of distinction, and surprise and new attack methods are seen as ways to create more casualties. One of the novel platforms that terrorists have been experimenting with to diversify and bolster their capabilities is drones (also referred to as uninhabited aircraft systems, or UASs, throughout this report). Four examples bring the utility, attractiveness and future potential of UASs as a platform for terrorists into focus.

In 1993, in preparation for an assassination plot against a rival leader, Aum Shinrikyo, a Japanese terror group motivated by an apocalyptic ideology, began experimenting with a new way to deliver sarin gas. The new delivery mechanism was a remote-control helicopter. Although the group never used the helicopter during an operation, it did conduct a successful attack against Tokyo's subway system using that same poisonous substance less than two years later. Then, two and half years after that incident, in 1997, in another part of the globe, a small group of elite Israeli commandos were finalizing their preparations for a sensitive operation they were about to conduct inside Lebanon, in a town called Ansariya. After disembarking from their entry craft and on their way to their objective, the Israeli team was ambushed by local fighters loyal to the Shi`a militant group Hezbollah. The fighters knew the Israeli commandos were coming, and they had been waiting for them, because for months prior Hezbollah had been able to gain access to and observe Israeli UAS feeds, which at the time were not well encrypted. Less than a decade after that surprise event, Hezbollah flew its first UAS across Israel's border. It was 2004.

Four years later, in December 2008, another important step was taken several thousand miles away by a private citizen in the United States. Jim Simmons, a hobbyist, attached a handgun to an over-the-counter remote-control helicopter he had purchased, and he successfully fired the weapon while the device was in flight. Not to be outdone, a teenager in Connecticut mounted a homemade, workable flamethrower to a small UAS seven years later, in 2015, upping the ante of what was possible with a little ingenuity even further. To the casual observer, these four events may appear distinct—and in many ways they are—but to a violently motivated terrorist group that seeks out publicity and novel ways to inflict harm on innocents, they likely tell a different story. To put it simply, these two private cases highlight options beyond what other terrorist entities have already proven. And in doing so, they demonstrate additional capability, show what can be replicated, and illustrate what, with a little imagination, lies within the realm of immediate terrorist possibility.

This study examines the evolution of terrorists' interest in and use of drones, and in doing so it provides unique insights into the threat posed by terrorists' use of this technology. This paper is organized into two parts. Section I provides an overview of the benefits of drones to terrorist groups and includes an analytical framework to situate their use. Through an investigation of terror-linked UAS cases, it also demonstrates how terrorists have sought to use UASs as an offensive platform. Section II broadens the aperture of analysis even further and reviews instances in which private citizens, who did not have violent intent, demonstrated additional UAS capability that could be mimicked or repurposed by those who embrace violence as a means to achieve political change. The report closes with a brief overview of emerging technologies that will likely further complicate future terrorist use of drones, and details the scope of this developing threat.

1 Brian Michael Jenkins, *The New Age of Terrorism* (Santa Monica, CA: RAND Corporation, 2006), p. 119.

2 For example, see "Iraq Sees Worst Bombing Since Invasion with 250 Deaths," BBC, July 6, 2016; Taylor Berman, "Graphic Execution Video Shows ISIS Drowning, Immolating Prisoners," Gawker, June 23, 2015.

UAS Research in Context

As aptly put by Dan Gettinger and his colleagues at the Center for the Study of the Drone, "Drones court controversy. Questions of privacy, human rights, and safety accompany the drone wherever it goes, from the backyards of private users to the battlefields of Afghanistan."[3] While interest in UASs has been wide, research into drones has mostly either been state-centric, dominated by the moral, ethical and legal questions regarding the use of military-grade platforms, or individual-based, revolving around questions of privacy. One major line of research inquiry centers on how UASs can or should be used (i.e., who can be snooped or targeted, where and how) and by whom (i.e., which entities have the authority to use drones, how their use should be regulated and under what conditions).[4] Two of the most contentious questions in this area involve the United States' use of "signature strikes"–strikes that are predicated on an observed pattern of behavior or other indicators as opposed to a specific person, or collection of people, being singled out due to intelligence—and the intentional targeting of American citizens by the United Sates government via armed drones.[5] Another major line of research, also legal and ethical in character, focuses on the death of innocent civilians and the collateral damage caused by armed UAS strikes.[6] Yet another area of research looks at the issue of privacy.[7] A fifth line of inquiry seeks to address such questions as how the increased use of border-crossing UASs by state actors affects or infringes on the other state's sovereignty, and potentially erodes that legal norm as a result.[8] Cross-cutting these avenues of research are questions that aim to provide insight into the proliferation of UASs, how effective their armed variants are, and the role drones and their associated technologies will play as a drivers, or change enablers, in the future of modern warfare.[9] Over the last several years, academic research has also focused on how drones can be used for good by nonstate actors.[10]

With some notable exceptions, less attention has been given to the use of drones by violent nonstate actors, and especially by insurgent and terrorist groups. One of the first individuals to comment publically on the attractiveness of UASs to terrorist groups was Christopher Bolkcom, an employee of the U.S. Congressional Research Service, who in July 2002 devoted a significant portion of his testimony

3 Dan Gettinger et al., *The Drone Primer: A Compendium of the Key Issues*, (Annandale-on-Hudson, NY: Bard College, Center for the Study of the Drone, 2014), p. 30.

4 For example, see Greg Miller, "Under Obama, an Emerging Global Apparatus for Drone Killing," *Washington Post*, December 27, 2011; and Greg Miller, "US Government's Refusal to Discuss Drone Attacks Comes under Fire," *Washington Post*, April 24, 2015.

5 On "signature strikes," see Kevin Jon Heller, "'One Hell of a Killing Machine': Signature Strikes and International Law," *Journal of International Criminal Justice* 11:1 (2013): pp. 89–119; on drones targeting American citizens, see Mark Mazzetti, "Killing of Americans Deepens Debate over Use of Drone Strikes," *New York Times*, April 23, 2015; and Scott Shane, *Objective Troy: A Terrorist, a President, and the Rise of the Drone* (New York: Tim Duggan Books, 2015).

6 For example, see "Get the Data: Drone Wars," Bureau of Investigative Journalism.

7 For background, see Wells C. Bennett, *Civilian Drones: Privacy, and the Federal-State Balance* (Washington, D.C.: Brookings Institution, Center for Technology Innovation, September 2014).

8 For example, see Daniel Brunstetter and Meghan Braun, "The Implications of Drones on the Just War Tradition," *Ethics and International Affairs* 25:3 (Fall 2011): pp. 337–58.

9 On state-focused drone proliferation, see Michael C. Horowitz and Matthew Fuhrmann, "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles" (unpublished paper, October 1, 2015); and Michael C. Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, "The Consequences of Drone Proliferation: Separating Fact from Fiction" (unpublished paper, January 25, 2016); on the effectiveness of drones, see Bryan C. Price, "Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism," *International Security* 4:36 (Spring 2012): pp. 9–46; Jenna Jordan, "Attacking the Leader, Missing the Mark," *International Security* 38:4 (Spring 2014): pp. 7–38; Michael J. Boyle, "The Costs and Consequences of Drone Warfare," *International Affairs* 89:1 (January 2013): pp. 1–29; Patrick B. Johnston and Anoop K Sarhabi, "The Impact of U.S. Drone Strikes on Terrorism in Pakistan," *International Studies Quarterly*, January 2016, pp. 1–17; on drones, emerging technology and the future of warfare, see Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Press, 2009); John Waters, "Next Generation Drone Warfare: An Interview with Paul Scharre," Real Clear Defense, February 24, 2015.

10 For example, see Austin Choi-Fitzpatrick, "Drones for Good: Technological Innovations, Social Movements and the State," *Journal of International Affairs* 68:1 (Fall 2014).

to a U.S. Senate committee to the topic.[11] In his briefing, Bolkcom identified seven features that made cruise missiles and unmanned aerial vehicles attractive to terrorist groups. These included low acquisition costs, a variety of purchasing pathways, potential for high accuracy, operational flexibility, a high likelihood of air-defense penetration, high survivability prelaunch and low levels of infrastructure needed to support their deployment.[12]

Bolkcom's remarks were followed soon thereafter by a short article titled "A Remote Threat" published by Michael Gips in the October 2002 issue of *Security Management*, which sought to sketch instances of terrorist interest in or use of UAS, and by extension examine the threat posed by this type of system. For that article, Gips interviewed Louis R. Mizell, a former U.S. intelligence officer who had created a list of all the incidents of terror interest in or use of remote-control technology that he could find. According to the data Mizell was able to compile, by October 2002 there had been "43 cases involving 14 terrorist groups in which remote-control delivery systems were either threatened, developed, or actually utilized."[13] As detailed in section I, some of these cases involved what we today call drones.

Covering different angles of this phenomenon, the researchers Dennis Gormley and Eugene Miasnikov added to this nascent base of literature through papers they published in 2003 and 2005 respectively.[14] Gormley identified the importance of two factors, a terrorist group's motivation and its capabilities, as being central to evaluating the threat posed by the terrorist use of UASs. He hypothesized that terrorist groups that are less interested in political compromise, and whose members are willing to die, are more likely than other terrorists to seek out weapons of mass destruction (WMDs) and platforms (i.e., cruise missiles and UASs) that can deliver them.[15] Gormley also outlined two creative ways, converting either an antiship cruise missile or a small plane, that terrorists could use to facilitate these types of attacks.[16]

Miasnikov's contributions to the literature were much more technical. In his 2005 report, Miasnikov sought to evaluate the potential damage a terrorist attack that incorporated a modified cruise missile or UAS might cause. He found that "even a small payload—of just a few kilograms—is capable to [*sic*] cause substantial damage."[17] He also identified four ways through which terrorist groups could acquire UAS. These included obtaining a military-grade UAS via theft or other means; purchasing a commercial UAS variant; building a device from scratch; and converting a small plane into an uninhabited system.[18] An appendix included in Miasnikov's paper also provided a listing of terrorist UAS use cases; several recent studies of the topic have used this list as a basis for analysis.[19]

Then, in 2008, Brian Jackson and other researchers from the RAND Corporation published a deep, landmark investigative study titled *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*, which sought to make sense of all of the work that preceded it, and of

11 Christopher Bolkcom before Senate Governmental Affairs Committee, Subcommittee on International Security, Proliferation, and Federal Services, Hearing on Cruise Missile Proliferation, 108th Congress, 2nd session, June 11, 2002, pp. 1–9.

12 Ibid., pp. 1–7.

13 Michael Gips, "A Remote Threat," *Security Management* 46:10 (October 2002).

14 Dennis Gormley, "UAVs and Cruise Missiles as Possible Terror Weapons," in Clay Moltz, ed., *Missile Proliferation, Missile Defenses* (Monterey, CA: CNS Occasional Paper no. 12, 2003); Eugene Miasnikov, "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects," Center for Arms Control, Energy, and Environmental Studies, Moscow Institute of Physics and Technology, 2005.

15 Gormley, "UAVs and Cruise Missiles as Possible Terror Weapons," pp. 4–5.

16 Ibid, pp. 5–7.

17 Miasnikov, "Threat of Terrorism Using Unmanned Aerial Vehicles," p. 5.

18 Ibid., p. 9.

19 Researchers at the Institute for Defense Analyses provided a similar summary and review of early terror UAS incidents in a publication released in October 2005. See Jay Mandelbaum et al., "Terrorist Use of Improvised or Commercially Available Precision-Guided UAVs at Stand-Off Ranges: An Approach for Formulating Mitigation Considerations," Institute for Defense Analyses, October 2005.

the threat that potential UASs and cruise missiles hold as a terrorist weapons system.[20] Building on Bolkcom's work, these researchers found that UASs are attractive as a platform for terrorists because they provide five operational benefits. These include (1) UASs' enabling attacks over national borders and perimeter defenses (2); the ability of a group to deploy multiple drones to support either (3) a multipronged assault or (4) a campaign of attacks over time; and (5) potential UAS hold as a mechanism to distribute WMDs.[21] Based on an analysis of UASs in relation to other weapons systems, such as guns and bombs, Jackson and his colleagues also found that UASs did "not appear to have major advantages over other ways of carrying out operations against similar targets, although they cannot be dismissed outright as a potential threat."[22] In their view, the UAS terror threat constituted a "niche threat," one that would be pursued on occasion, but would not replace simpler alternatives.[23]

A steady stream of news reports and shorter analytical pieces on the topic has continued since. Starting in the summer of 2015, at least four major reports that touched on various facets of the "terrorist use of UAS" issue were released, resulting in what one might characterize as a second round of substantive research on the topic. These releases include Kelley Sayler's June 2015 study for the Center for a New American Security (CNAS); Robert J. Bunker's August 2015 report published by the U.S. Army War College; the Remote Control Project's January 2016 release; and a paper authored by researchers affiliated with Armament Research Service in February 2016.[24]

Sayler's report adds value to the existing literature through an overview of the capabilities of four different types of UAS systems ranging from simpler and more accessible "hobbyist" variants to highly advanced and sophisticated military stealth drones. The report released by CNAS is also unique given its examination of the potential that small, commercially available UASs hold for overmatch against more capable (typically state) adversaries.[25] Robert Bunker provides a more detailed and granular look at the terrorist use of UASs, and his report contributes to our understanding of this phenomenon in three main areas. First, building on the work done by Gips and Miasnikov, Bunker provides a more complete list of suspected UAS terror use cases.[26] While this list is useful, and it represents a step forward, a number of the cases included on it either did not transpire or are misattributed, factors that limit its value. Second, Bunker outlines a number of different ways that UASs can be used by terrorists, and he offers categories to help situate UAS incidents.[27] Third, Bunker's piece provides threat-projection scenarios that evaluate future terrorist use of UASs along three dimensions: a UAS attack involving a single piloted system, an operation executed using a group of piloted and semiautonomous UASs and an incident that involves a networked and autonomous UAS swarm.[28]

The Remote Control Project's contribution to the literature lies in its assessment of the capabilities (payload, range, weatherproofing and sensors) of a number of commercially available drones, and in

20 Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles* (Santa Monica, CA: RAND Corporation, 2008); Another study that was released around this time, after the RAND report, was Ajay Lele and Archana Mishra, "Aerial Terrorism and the Threat from Unmanned Vehicles," *Journal of Defence Studies* 3:3 (2009).

21 Jackson et al., *Evaluating Novel Threats to the Homeland*, pp. xv, 27–61.

22 Ibid., pp. xv–xvi.

23 Ibid., p. xvi.

24 Kelley Sayler, *A World of Proliferated Drones: A Technology Primer* (Washington, D.C.: Center for a New American Security, June 10, 2015); Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications*, (Carlisle, PA: U.S. Army War College, August 2015); Chris Abbott et al., "Hostile Drones: The Hostile Use of Drones against British Targets," Remote Control Project, January 2016; Larry Friese, N.R. Jenzen Jones and Michael Smallwood, "Emerging Unmanned Threats: The Use of Commercially-Available UAVs by Armed Non-State Actors," Armament Research Services, Special Report no. 2, 2016.

25 Sayler, *World of Proliferated Drones*, p. 29.

26 Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles*, pp. 7–15.

27 Ibid., pp. 16–24.

28 Ibid., pp. 24–33.

its documentation of UAS use incidents from a broad range of nonstate actors.[29] Armament Research Service's report provides value by documenting the variety of ways drones have been used by nonstate actors, and in its finding that UAS use is not limited to a specific geographical area or ideological group type.

Similar to the work done by Brian Jackson and his colleagues in 2008, the current report aims to draw from the existing body of literature and to enhance it by adding value in several key areas. First, since a number of alleged UAS terror cases have either been disproven or lack adequate sourcing, the author aims to create a more firmly rooted historical baseline, so that analysts and policymakers alike can better distinguish fact from fiction, and track the future evolution of this issue moving forward.[30] Second, while most authors of similar studies have provided typologies of UAS type, none has yet to incorporate a UAS terrorist use typology, a feature that this study includes. Third, by distinguishing between terror entities that have shown a more limited interest in UASs and those whose UAS use is sustained and developed enough to be considered a "program," this study aims to elevate the discussion of this phenomenon beyond one-off cases to a consideration of what is, at least for some groups, a more structured, integrated and resourced capability. Fourth, by including a review of innovative drone uses by private civilians who do not have violent intent, the author seeks to develop a more accurate picture of what is currently possible when that type of proven use is mirrored, mimicked or modified by entities that embrace terrorism as a methodology.

Scope, Methods, Sources and Caveats

The author recognizes that terrorist use of drones is only one dimension of a much larger issue: terrorist use of robotics and remote-control and autonomous systems on the land, at sea and in the air. Terrorists of various stripes have long used remote-control technology to detonate bombs and inflict harm in other creative ways, but for the sake of clarity (and brevity), this study focuses on UAS use exclusively. Second, while the author has gone to great lengths to investigate all UAS terror incidents and assemble as complete a list as possible, the cases reviewed in this paper are those that were found to be credible and occurred before mid-October 2016. Incidents involving insurgent groups' use of UAS, such as the cases associated with several armed Libyan or Syrian-based rebel groups, were not included.[31] Owing to the secrecy surrounding terrorist organizations, and to state efforts to combat them, the material in this paper should not be read as a full catalog of all terror-linked UAS cases. While this report would significantly inform such an effort, that type of endeavor is beyond the scope of this study. Further, while this report provides a framework to situate terror UAS use, it should not be read as a full representation of all of the individual ways that terrorists can use drones. Given the multiplicity of do-it-yourself (DIY) approaches and creative ways to use drones, such an approach would not be well conceived. Lastly, owing to security concerns, a broad and comprehensive examination of anti-UAS countermeasures is also beyond the scope of this report.

---

29 Abbott et al., "Hostile Drones," pp. 4–6, 10–13.

30 The most problematic terror UAS cases covered in these two reports include a rumored al-Qa`ida plot against the U.S. president and other world leaders at the G8 summit in Italy in the summer of 2001; an anthrax plot that reportedly involved Mozzam Begg, a former Guantanamo Bay prison inmate; and an alleged al-Qa`ida plot from the 2002 period that involved targeting civilian airliners. The author has decided to not include these cases because they either have been disproven or lack enough evidence to warrant inclusion.

31 For example, incidents involving Libyan rebels from Misrata were not included (see Spencer Ackermann, "Libyan Rebels Are Flying Their Own Mindrone," *Wired*, August 23, 2011), and incidents involving the Mujahidin Shura Council of Darna (Libya) were also not included (see Thomas Joscelyn, "Islamic State Concedes That Fighters Retreated from Derna, Libya," ThreatMatrix blog, April 22, 2016); the same applies to the Syrian group Ahrar al-Sham, for background on that group's use of an explosive laden drone see the video embedded in Thomas Gibbons-Neff, "ISIS Used an Armed Drone to Kill Two Kurdish Forces and Wound French Troops, Report Says," *Washington Post*, October 11, 2016. Cases associated with these latter two groups have not been included, as although these groups have operated with terror groups, their targets are primarily state elements or other rebel or terrorist groups, and not civilians.

Sections I and II were written using a case study approach, and they incorporate a broad range of sources that the author found online. Any other limitations or errors associated with this report are the author's alone.

Terms and Types of Platforms Discussed

The term "uninhabited aircraft system(s)" was purposefully chosen over other options, including "drone," "unmanned aerial vehicle," "remotely piloted aircraft," and other terms for a number of reasons. First, "drones" are not limited to the aerial domain, as "drones" can be used—and are being used—for underwater and ground applications.[32] The term "drone" also carries negative and positive connotations, which, depending on the reader, could serve as a distraction.[33] Second, the author believes that the use of term "unmanned aerial vehicle" is somewhat misleading, because even though these systems will soon be able to operate autonomously, their most common usage today involves human-machine teaming and the control of the system by a human operator via remote control. It is true that the platforms themselves are not guided by a pilot who is physically sitting in the system and are therefore "unmanned," but the majority of these systems—at least today—are controlled by a human pilot operating from a stand-off distance. The term "remotely piloted aircraft" suffers from a similar limitation, as this usage implies that the aircraft must be remotely controlled, and it implies that the vehicle does not have autonomous capabilities. Due to these reasons, the author believes that "uninhabited aircraft system(s)" is the term that creates the least amount of confusion regarding the issue being studied. The term "drone" is also used throughout to ease this report's readability.

Another important distinction that needs to be drawn are the types, or classes, of UASs that are studied in this report. Indeed, as noted by Lynn E. Davis and her RAND colleagues, "armed UAVs vary in size, range, payload, lethality, and complexity, and categorizing these systems is important for understanding who is interested in them, for what purpose, [and] how dangerous they are."[34]

To prevent the proliferation of sensitive nuclear-capable missiles and related technology during the Cold War, the United States and several other countries established the Missile Technology Control Regime (MTCR).[35] The MTCR has evolved since that time, and today it also governs the transfer or sale of UASs and related technology, based on a two-tiered classification system.[36] The first category concerns "Category I" systems, which are defined as being "capable of delivering a payload of at least 500 kg to a range of at least 300 km, and their major complete subsystems, production facilities, and related technology."[37] These types of systems are predominately large, sophisticated military-grade UASs, and they do not feature in this report (because evidence has not emerged that terrorist entities possess or have used this type of system). The other category covered by the MTCR are "Category II" systems, which "include materials that are less sensitive but still capable of covering a range of 186

32 For example, see Ari Daniel Shapiro, "Remotely Piloted Underwater Glider Crosses the Atlantic," *IEEE Spectrum*, February 26, 2010.

33 For example, as noted by the Center for the Study of the Drone, "the use of the word 'drone' is itself a matter of heated debate. If you search for the word 'drones' on Twitter, you'll see a conversation that is largely dominated by antidrone and drone-neutral sentiments. None of the big defense and aviation companies use the word. But if you look up 'UAV'—which stands for Unmanned Aerial Vehicle—the feed is largely dominated by tech companies and drone advocates sharing news about developments in the field. These two conversations are essentially happening in isolation of each other: head-on engagement is therefore difficult." See Gettinger et al., *Drone Primer*, p. 31.

34 Lynn Davis and her colleagues at RAND have also developed a useful typology for armed UAVs. See Lynn E. Davis et al., "Armed and Dangerous: UAVs and U.S. Security," RAND, May 1, 2012, p. 9.

35 For background, see Bureau of International Security and Nonproliferation, "Missile Technology Control Regime (MTCR)," Fact Sheet, March 4, 2009; and Sarah Kreps, *Drones: What Everyone Needs to Know* (New York: Oxford University Press, 2016), pp. 13–16.

36 In precise terms, the MTCR "restrict[s] transfers of 'missiles'—defined as rocket systems (including ballistic missiles, space launch vehicles, and sounding rockets) and unmanned aerial vehicle (UAV) systems (including cruise missiles, target drones, and reconnaissance drones) capable of delivering weapons of mass destruction (WMD)—and their related equipment and technology." See Bureau of International Security and Nonproliferation, "Missile Technology Control Regime."

37 Bureau of International Security and Nonproliferation, "Missile Technology Control Regime."

miles, irrespective of payload, and have less stringent export prohibitions."[38] As noted by Sarah Kreps, "an example [of a Category II system] includes Iran's Ababil, a reconnaissance, surveillance, and attack aircraft that has a payload of 40kg (or about 88 lb.) and is thought to be the system exported to Hezbollah and potentially Venezuela."[39] Smaller and less-capable UASs that do not fit within the MTCR classification scheme "fall outside of the MTCR altogether—meaning they can be exported" with much less, or without any, scrutiny.[40]

The U.S. Army uses a five-tiered classification system to categorize UASs. This classification system ranges from Group 1 UASs (the smallest variants), which are hand-launched, highly portable systems that have very limited range and endurance, to much more sophisticated Group 4 and 5 systems.[41] These two latter categories include machines like the Predator that operate at medium to high altitudes, have extended range and endurance and are able to carry and fire several large munitions.

A more helpful categorization is one developed by Kelley Sayler at the Center for a New American Security. In her report *A World of Proliferated Drones: A Technology Primer*, Sayler identifies four UAS types: hobbyist drones, midsize military and commercial drones, large military-specific drones and stealth drones.[42] This report borrows these categorizations and focuses on the first two—hobbyist drones and midsize military and commercial drones—as they are the UAS types that have been used by, and are currently most accessible to, terrorist entities. Sayler defines the key attributes of these two types as:

> **Hobbyist Drones**
>
> Readily available for purchase—generally for no more than a few thousand dollars—by any interested party. These systems may either be pre-assembled or assembled from component parts and do not require formal infrastructure or training to operate. Current commercial off-the-shelf technology enables hobbyist drones to perform aerial surveillance or deliver payloads—including explosives or chemical or biological agents—of a few kilograms at ranges up to a few kilometers.
>
> **Midsize Military and Commercial Drones**
>
> Those that are not generally available to individuals due to cost or infrastructure requirements. These systems may, however, be sold or transferred to foreign militaries and non-state actors [with appropriate export control waivers]. While these systems are generally used for surveillance purposes at present, they are likely to be increasingly armed, either with an explosive payload that can perform a kamikaze mission or, in time, with releasable precision-guided munitions.[43]

Figure 1 provides an overview of the MTCR, U.S. Army and CNAS classification schemes, and it details the categories or group of UAS from each matrix that feature in and are reviewed as part of this report. Other, more granular UAS classification schemes can also be found in the appendix.[44]

38 Kreps, *Drones*, p. 14.

39 Ibid.

40 Ibid.

41 For a review of specific differences between these groups, see *"Eyes of the Army:" U.S. Army Unmanned Aircraft Systems Roadmap (2010–2035)*, (Fort Rucker, AL: U.S. Army UAS Center of Excellence), pp. 12–13.

42 Sayler, *World of Proliferated Drones*, pp. 5-6, 8. Another useful typology that other researchers have used is dividing drones into tactical, armed and advanced categories. See Horowitz and Fuhrmann, "Droning On," pp. 15–16; for general background, see Friese et al., "Emerging Unmanned Threats," pp. 14–20; for a typology of armed UAVs and "other" drones, see Davis et al., "Armed and Dangerous," pp. 2–4; for a more technical typology, see "Joint Doctrine Note 2/11: The UK Approach to Unmanned Aircraft Systems," March 30, 2011, pp. 2-4–2-6.

43 Sayler, *World of Proliferated Drones*, pp. 5–6.

44 See also the breakdown provided by "1.4 Classification of the Unmanned Aerial Systems" at www.e-education.psu.edu/geog892/node/5.

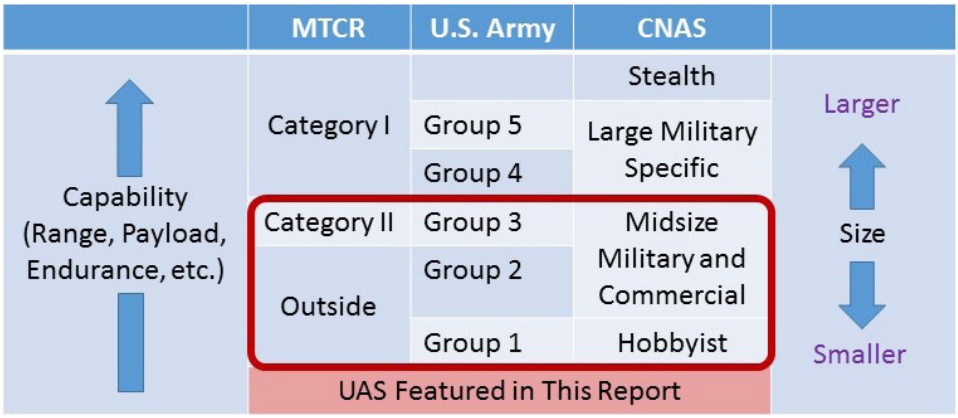

Figure 1: Breakdown of UAS Types Reviewed across MTCR, U.S. Army and CNAS Classification Schemes

Section I: Capabilities and Potential—Terrorists' Interest in and Use of UASs

With the availability of these great inventions, there is only one thing left, which is the unmanned aerial vehicle. It is the sought hope and the unachieved dream.…

Why don't the brothers build planes like these or buy them from the market, load them with explosives and target military bases, or even develop these planes; and make them fly for longer distances? These planes can be the best supporters for mujahidin and they can easily found from toy stores.

—Abu `Ubayda al-Maki, 2012[45]

The 2012 quotation from Abu `Ubayda al-Maki that opens this section illustrates that just as UASs are an attractive technology for state actors, they are also attractive to, and sought after by, terror groups and those inspired by them. Given the benefits of UAS technology, terror groups' use of drones is a predictable problem. For example, before the summer of 2013, Eric Schmidt, Google's former chief executive officer, and Dennis Blair, the former U.S. director of national intelligence, both predicted that terror groups' use of UASs would soon be an issue.[46] A number of terrorist groups had already shown interest in or had used UASs at least a decade prior to 2013, proving that terror groups' interest in this technology was far from new. By cataloging instances in which terrorist actors have used drones, this section provides insights into terrorist capability and decisionmaking. To contextualize the issue, section I begins with an overview of the factors that make drones attractive to terrorist organizations, and to those who take steps toward violent action on their behalf. It then provides a typology against which both threats and the current and future instances of terror use of UAS may be evaluated. To exemplify this typology, an overview of historical and contemporary instances in which terror groups, or individuals motivated by them, have demonstrated either an interest in UASs or a certain level of UAS capability follows. Only those terror-linked UAS cases that the author found and assessed to be credible were included.

Benefits, Unique Characteristics and Attractiveness of UASs

Drones are attractive to terrorist groups for a number of reasons.[47] As noted by Brian A. Jackson et al., the advantage of UASs "over other attack modes" lies "not in the destructive power that they can carry… [but] in the way they carry that power and the distance from which they allow an adversary to control its delivery."[48] The two primary ways that UASs do this is by enabling aerial operations and by enhancing an attacker's ability to project force over longer distances, and in doing so extend the UAS controller's stand-off distance from the target.[49] Again as noted by Jackson et al., depending on the range and sophistication of the device being used, UASs have the potential to "allow attacks to be

45 Abu `Ubayda al-Maki, "Al-Qa`ida and Its New Project: A UAV," Al-Fida', May 2012.

46 "The Rise of Robot Wars," *Daily Mail*, April 12, 2013; David Wood, "Armed Drones Could Target President," Huffington Post, January 22, 2013.

47 For a great overview of this issue, see Statement of Christopher Bolkcom before Senate Governmental Affairs Committee, Subcommittee on International Security, Proliferation, and Federal Services, Hearing on Cruise Missile Proliferation, June 11, 2002, pp. 1–9; see also Jackson et al., *Evaluating Novel Threats to the Homeland*, p. xv; see also Horowitz, Kreps and Fuhrmann, "Consequences of Drone Proliferation," pp. 15–18; and Eugene Miasnikov, "Non-State Actors and Unmanned Aerial Vehicles" (presentation at ISODARCO XXVI Winter Course, "New Military Technologies: Implications for Strategy and Arms Control," 6–13 January, 2013, Andalo, Italy), pp. 19–23.

48 Jackson et al., *Evaluating Novel Threats to the Homeland*, p. xv.

49 For background on the aerial advantage of UASs and their benefit from a stand-off perspective, see ibid. and John. P. Abizaid et al., "Recommendations and Report on the Task Force on US Drone Policy," (Stimson Center, second edition, April 2015).

staged by teams at a considerable distance from the target site."[50] For more-capable UAS variants, this potential could include the device's being controlled by a cell located across an international border or on a body of water, which would naturally complicate or delay any local response.[51]

For those terror organizations with less-robust UAS platforms and know-how, one of the main benefits of commercially available UASs is their accessibility and low start-up cost. Basic UAS platforms with cameras, GPS technology and other sensors are relatively cheap and easy to purchase, use and transport; all of which give a terrorist operative flexibility and mobility, making his or her actions—even if small in scale and of limited impact—hard to predict and detect.[52] The pace of innovation and technological change over the next decade and the capabilities of commercially available UAS platforms and sensors will only grow and intensify.[53]

Another key complicating factor is that the main driver of that change will be the private sector, and not, as it has been in the past, the U.S. defense establishment.[54] This means that in the future we are likely to see a further democratization of UASs and associated sensor technology, which, depending on the user of that technology, can have both positive and negative effects.[55] The danger to nation-states is that the availability of UASs and their sensors will led to new innovations in use driven from below by a DIY movement that favors spontaneously creative experiments versus those arising from institutions with more resources. Such a playing field favors those actors, as demonstrated by al-Qa`ida on 9/11, who seek out and try to exploit bureaucratic and other seams, and that have the agility to do so. This is a future for which some argue that the U.S. defense establishment is not well prepared. As noted by Paul Scharre, "the U.S. military is used to competing in a world where some of the most game-changing innovations—such as stealth, GPS and precision-guided weapons—come from the U.S. defense sector. It is ill-prepared for a world where such technologies are widely available to all."[56]

Another major factor that makes drones attractive to terrorists is the fear that they inspire. This takes place across a number of different levels. First, drones, at least to some extent, challenge existing physical security paradigms.[57] For example, given the threat of penetration or attacks by air, facilities that were once hardened and difficult to penetrate due to stand-off barriers and other security checks may no longer be as safe as they were previously.[58] This includes national borders, as the portability and small-scale signatures of commercially available UASs also challenge conventional views on air defense and how nation-states have approached that issue. UAS penetration of sensitive facilities like the White House complex or a nuclear facility (both of which have already taken place), are embarrassing and result in additional publicity for the entity responsible, even if no attack occurs.[59] Second, UASs have the potential to provide greater intimacy and closeness to a target, potentially contributing to

50 Jackson et al., *Evaluating Novel Threats to the Homeland*, p. 28.

51 Ibid.

52 Some have characterized this benefit as "increased optionality." See *Game of Drones: Wargame Report*, (Center for a New American Security, June 29, 2016); for an overview of the sensors and technology available on commercial UAS platforms, see Larry Friese, et al., "Emerging Unmanned Threats: The Use of Commercially-Available UAVs by Armed Non-State Actors," Armament Research Services, February 2016, pp. 24–25.

53 For background, see "UAV Payload Market Size to Reach $6.34 Billion by 2022," Grand View Research, January 2016.

54 "Joint Doctrine Note 2/11," pp. 6–13; Paul Scharre, *Robotics on the Battlefield, Part 2: The Coming Swarm*, (Washington, D.C.: Center for a New American Security, October 2014), p. 42.

55 There is an abundance of ways that UASs can be used for good. For example, commercially available UAS platforms have already proved useful to search-and-rescue operations. For other applications, see the Drones for Good Project webpage.

56 Scharre, *Robotics on the Battlefield, Part 2*, p. 11.

57 For background, see John Villasenor, "The Drone Threat to National Security," *Scientific American*, November 11, 2011.

58 Ibid.

59 For a richer treatment of these incidents, see Michael D. Shear and Michael S. Schmidt, "White House Drone Crash Described as a U.S. Worker's Drunken Lark," *New York Times*, January 27, 2015; and "Who Is Flying the Mystery Drones over France's Nuclear Sites?" BBC, October 31, 2014.

greater accuracy, which also results in the shrinking of areas once considered safe. Third, and perhaps most significant, is the multiuse potential of drones, given the cameras with which many are equipped, whereby a UAS can function as both an attack platform and as a mechanism for a terror group to document, or to self-publish, the potential assassination of an individual or the death of a small group in gruesome and close detail. One has only to look at the horrific assassination in 2015 of a local U.S. news reporter and her cameraman while conducting an interview on live TV by a former disgruntled colleague to see the potential, as the assassin took a first-person point-of-view video of the gun attack (showing the perspective of the shooter) during that incident, which he later uploaded to YouTube.[60] If used in a similar way, drones have the ability to extend both one's virtual and physical presence.[61]

For some groups, the novelty and symbolic significance of attacking the United States or the West with drones—technology pioneered in the West—also likely adds to their attractiveness. As noted by Lynn E. Davis et al:

> The novelty of the method might appeal to al Qaeda's leaders, demonstrating their cleverness and raising the psychological impact of the strike. Given the devastation that drones have wrought on al Qaeda's leadership, the symbolic value of giving America a taste of its own medicine might be appealing and powerful. They may reason, correctly, that the specter of "death from above" might discomfit many Americans, maximizing the psychological impact, as well as any associated coverage of a strike. Al Qaeda could also strike at targets with guarded perimeters and evade these defenses.[62]

Drones also provide other benefits. For example, drones, like suicide bombers or other forms of improvised explosive devices, could also be used to channel or draw people to (or out of) a specific location, making those people more vulnerable to a secondary or follow-on attack.[63] Drones also provide a loitering capability, allowing operators to maintain "eyes" on a target for an extended period. As a drone wargame conducted by the Center for a New American Security revealed, the loitering capability of drones can also be used to enhance traditional weapons systems, such as the firing and accuracy of unguided rockets.[64]

An Analytical Framework

This study includes a typology to help the reader make sense of the incidents in which terrorists have used drones. The typology draws from existing frameworks used by both academics and the U.S. government, and it was developed based on conversations with U.S. interagency personnel.[65] As illustrated in figure 2, the typology is broken into three main categories that increasingly provide more detail about how a UAS is used, or could be used, as one moves across the typology from left to right.

60 For background on the incident, see Ashley Fantz and Jason Hanna, "Virginia Journalists' Slayings: Man Thought to Be Ex-Station Employee Shoots Self," CNN, August 26, 2015; for a link to the shooter's video, see http://heavy.com/news/2015/08/vester-lee-flanagan-bryce-williams-pov-shooting-murder-video-twitter-tweet-youtube-video/.

61 Lev Grossman, "Drone Home," *Time*, February 11, 2013. The author of this piece had a similar view: "A drone isn't just a tool; when you use it you see and act through it—you inhabit it. It expands the reach of your body and senses in much the same way that the Internet expands your mind. The Net extends our virtual presence; drones extend our physical presence. They are, along with smart phones and 3-D printing, one of a handful of genuinely transformative technologies to emerge in the past 10 years."

62 Davis et al., "Armed and Dangerous," p. 12. As noted by Peter Singer, it would also be helpful if the United States avoids "'designer hubris': the assumption that just because one party is the first to develop a new technology that means that they will always be in control of the innovation, and their views and mores will be used to manage and guide its use forever." Peter Singer, "The Five Deadly Flaws of Talking about Emerging Military Technologies and the Need for New Approaches to Law, Ethics, and War," in Peter Bergen and Daniel Rothenberg, *Drone Wars: Transforming Conflict, Law and Policy* (New York: Cambridge University Press: 2015), p. 223.

63 For example, see Jackson et al., *Evaluating Novel Threats to the Homeland*, p. 24.

64 G*ame of Drones: Wargame Report*, pp. 4–8.

65 For other typologies of drone use, see Austin Choi-Fitzpatrick et al., *Up in the Air: A Global Estimate of Non-Violent Drone Use 2009–2015*, (University of San Diego, Joan B. Kroc School of Peace Studies, 2016), pp. 8–10.

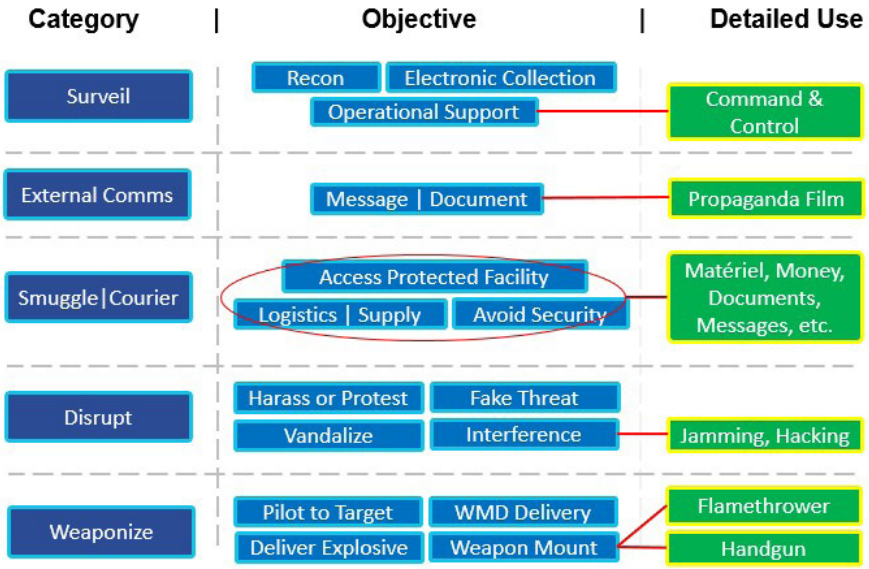

Figure 2: Typology of Terror UAS Use

The "category" column on the far left of figure 2 identifies the five broad ways UASs can be employed. This includes UASs being used for surveillance; for external communications or strategic messaging purposes; to smuggle matériel; to disrupt or sabotage an event; and as a weapon.

The middle column of the typology identifies the immediate objective associated with each corresponding category. Examples of these objectives are as follows:

- **Surveillance Objectives:** There are a number of ways that a terrorist organization could use a UAS to conduct surveillance. For instance, a UAS could be used to conduct reconnaissance around a terror group's location or a target in advance of an attack, for ongoing mission support during an operation (e.g., with the UAS providing a bird's-eye view of a battle) or as a rudimentary cyber surveillance platform to collect local electronic communications that are not well encrypted.
- **Strategic Communications Objectives:** As the Islamic State and others have already illustrated, drones can also be used to film and document operations. This information can then be exploited for propaganda purposes and included in videos released to the public as part of a group's external communications strategy.
- **Smuggle/Courier Objectives:** Drones can also be used by terrorist groups to smuggle or carry matériel into a protected facility, across a denied area (i.e. an international border or other sensitive location) and to ferry items (i.e., messages, money or phones) that might be too risky to send via human couriers.
- **Disrupt Objectives:** There are also a number of ways that drones can be used in a nonviolent manner as a form of disruption. These include using a UAS to carry out a protest or a high-publicity stunt, similar to the actions taken by the German Pirate Party when it flew a UAS over German chancellor Angela Merkel during an event. UASs can be used in a similar way to vandalize or deface property, or interfere with electronic communications, stunts that could garner publicity for a group.
- **Weaponize Objectives:** The most sinister category of UAS use is weaponizing the device, an objective that can be achieved a number of different ways. Perhaps the most intuitive method is to use the UAS to deliver or drop an explosive. A variant of this approach involves a controller loading a UAS with explosives and piloting the device directly to its target. Weapons, such as a handgun or flamethrower, can also be directly mounted to a UAS and then used to conduct an attack against

an individual or group at close range. Although technically much more difficult to achieve, aerosol or spraying devices can also be attached to a UAS to distribute chemical and biological agents. And, although technically a nonviolent use, a UAS could also be used to augment other weapons systems or as a diversionary device to channel a crowd to another location where attackers could be lying in wait.

Finally, the "detailed use" column on the far right of figure 2 provides even more specific information about UAS use in each category. This typology has been included to help the analyst and decisionmaker analytically categorize UAS incidents as they occur. It is not designed to be fully comprehensive.

UAS Cases: From Initial Innovation to Individual Users and Programs

For the sake of clarity, the subsection that follows is divided into two sections: individual cases and programs. This distinction has been made because available evidence indicates that four terrorist groups—Hezbollah, HAMAS, the Islamic State, and Jabhat Fateh al-Sham—have either used drones frequently enough, or have identifiable mid-to-long term infrastructure dedicated to supporting such operations, that their efforts warrant being labeled a "program." Even though many of the "individual" events that follow were associated with al-Qa`ida, or were led by individuals motivated by the ideology and goals of that group, the existing evidence more strongly supports these events as being a series of one-off events, rather than as being representative of a centrally coordinated and more bureaucratically robust program. It is certainly possible that other terrorist groups could have more-established programs, or are trying to create them. Indeed, it is widely known that a number of militant and insurgent actors in Syria and Iraq, like the Free Syrian Army and Ahrar al-Sham, have also used drones. The analytical decision to identify the four groups mentioned at the start of this subsection as those with dedicated programs was made based on open-source material available about this phenomenon at the time of writing.

Individual Cases

The first category of UAS use includes a mix of cases that are either tied to a specific terrorist group or are associated with individuals who were acting on their own behalf or in loose or unclear affiliation with a formal terror organization.[66]

AUM SHINRIKYO	1993–1994
Overview: UAS possession; flight tests conducted	

The first known instance of a terror group's interest in drones occurred in late 1993 and early 1994, involving the Japanese apocalyptic group Aum Shinrikyo, the entity responsible for the successful 1995 sarin gas attack against the Tokyo subway.[67] During that time, Aum Shinrikyo made at least two assassination attempts on the life of Daisaku Ikeda, the leader of the Buddhist group Soka Gakkai,

66 For good general background on many of the cases discussed in this section, see Paul Cruickshank and Tim Lister, "Terror and Toy Planes—not so Remote," CNN Security Clearance blog, August 7, 2012.

67 For background on Aum Shinrikyo, see David E. Kaplan and Andrew Marshall, *The Cult at the End of the World* (New York: Crown, 1996); for a historical list of manned "terrorist incidents involving the crashing of airplanes into targets," see Adam Dolnik, *Understanding Terrorist Innovation: Technology, Tactics and Global Trends* (New York: Routledge, 2007), pp. 39–40.

whom Shoko Asahara—the head of Aum Shinrikyo—despised.[68] Both attempts reportedly involved the use of sarin gas, and the sources are mixed regarding which dispersion methods were used for each attempt.[69] One account suggests that Aum Shinrikyo dispersed the sarin gas from trucks that had been converted for that purpose for both attempts. Multiple sources indicate, however, that while a UAS was not used during those attempts, Aum Shinrikyo did experiment with, and considered using, a remote-control helicopter as its attack platform.[70] According to a presentation given by Kyle Olson at a U.S. interagency event focused on chemical and biological terrorism in 1995, Aum Shinrikyo owned "a couple of remote control helicopters of the kind used in Japan for aerosol spraying of crops."[71] When the group was "asked by the vendor [from whom they were purchasing the devices] whether or not they wanted the spray tank attachments, they said, 'No we already have our own, thank you.'"[72] Aum Shinrikyo's goal was to attach an aerosol dispersion device to a remote-control helicopter so it could be used in the attack. Aum Shinrikyo is believed to have gone with the truck option instead because "the helicopters crashed during testing."[73] This case is the first known instance of a terrorist group attempting to use a UAS. It is also the first known attempt by a terror group to weaponize such a device.

Two terrorist groups to follow Aum Shinrikyo's interest in drones were the Colombian-based Revolutionary Armed Forces of Colombia (FARC) and the Pakistan-based Lashkar-e-Taiba. As detailed below, both of these groups showed an interest in and possessed UAS and associated technology in the years that immediately followed 9/11. Yet we know very little about how, when and where the two groups planned to use this technology.

FARC	2002
Overview: In possession of nine UASs; use unclear	

The only information that exists about the FARC case is that in August 2002, Colombian government forces raided a FARC camp and found "nine model airplanes that rebels were planning to fill with explosives and crash into government targets via remote control."[74] The suspected target, according the Colombian general in charge of the operation, was "an important oilfield in the area," which, if true, suggests that FARC potentially planned to use their UASs for an operation that was more akin to economic sabotage—similar to the arson and other sabotage-type attacks that are often affiliated with radical left-wing groups, like the Earth Liberation Front in the western United States.[75]

68 For background, see Richard Danzig et al., *Aum Shinrikyo: Insights into How Terrorists Develop Biological and Chemical Weapons*, 2nd edition (Washington, D.C.: Center for a New American Security, December 2012), p. 20; and T. Ballard et al., "Chronology of Aum Shinrikyo's CBW Activity," *CBW Activities* (Monterey Institute of International Studies), March 15, 2001.

69 See, for example, the two sources listed in note 68.

70 See Amy E. Smithson, "Rethinking the Lessons of Tokyo," in *Ataxia: The Chemical and Biological Terrorism Threat and the US Response* (Stimson Center, October 9, 2000), p. 80; Gordon C. Oehler (director, Nonproliferation Center, Central Intelligence Agency), "Testimony before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs," United States Senate, 104th Congress, 1st Session, November 1, 1995; Kyle Olson, "Overview: Recent Incidents and Responder Implications" (presentation and remarks given at the Responding to the Consequences of Chemical and Biological Terrorism Seminar, July 11-13, 1995), pp. 2–42; see also the sources related to this incident that are listed in Ballard et al., "Chronology of Aum Shinrikyo's CBW Activity."

71 Olson, "Overview," pp. 2–42.

72 Ibid.

73 Gips, "Remote Threat."

74 "Troops Seize Rebels' Explosive Planes," Houston Chronicle News Services, August 27, 2002.

75 Ibid. For background on the Earth Liberation Front, see the film *If a Tree Falls: A Story of the Earth Liberation Front*, January 2011.

LASHKAR-E-TAIBA	2002
Overview: Acquisition of, and experimentation with, range-extending UAS components	

In 2003, a group of friends residing in Virginia were charged with providing material support to the Pakistani terrorist group Lashkar-e-Taiba (LeT) and with attempting to join the Taliban so they could fight the U.S. forces in Afghanistan. Even though the larger conspiracy involved individuals outside the Virginia area, the group was dubbed the "Virginia Jihad Network" since most of the members of the cell resided in that state. Further, even though the group's members were formally charged in 2003, for some of the individuals involved (who were later convicted) the activity and associations they were prosecuted for reached back to 1999 and the days and months that immediately followed 9/11.[76] Ultimately, the case resulted in the successful conviction of at least nine cell members, including the group's spiritual adviser, who was serving as an imam at a mosque in Northern Virginia.[77]

Since the event occurred close to 9/11, and the cell was the largest jihadi clique to be disrupted in the United States at the time, the majority of media accounts highlighted the cell members' desire to receive military training and fight against U.S. troops aboard. Less attention was given to an equally sinister and dangerous dimension of this group's dealings: its acquisition of sensitive technology to assist and enhance the performance of UASs, and to do so on behalf of LeT. This case is important because it illustrates that LeT has been interested in acquiring drones and technology designed to boost their performance since at least early 2002, and that the group leveraged a network of U.S. residents to acquire this type of advanced technology directly from U.S. companies.[78] LeT's attempt to acquire UAS-affiliated technology is not that surprising, as an article published by the group in July 2000 claimed that LeT was already using UASs and had the capability to manufacture them.[79] Further, the Indian government has alleged that Pakistan, the historical sponsor of LeT, has since at least 1997 flown UASs into territory claimed by India.[80]

The UAS dimension of the Virginia Jihad Network primarily involved three individuals—the U.S. residents Ali Asad Chandia and Seifullah Chapman, and Mohammed Ajmal Khan, an LeT operative based in Britain.[81] While Khan was the driving force behind the acquisition of the sensitive technology and was the individual who dialoged with U.S. companies to acquire it, Chapman paid for some of the products, and Chandia supported Khan effort's to acquire and ship the matériel overseas.[82] Early on in the process, Khan disclosed to his fellow accomplices that he was purchasing the matériel for LeT.[83]

76 See Memorandum Opinion, *United States of America vs. Masoud Khan, et. al.*

77 See Jerry Markon, "'Va. Jihad Case' Hailed As Key in War on Terror," *Washington Post*, June 8, 2006.

78 For background, see Indictment, *United States of America vs. Ali Asad Chandia and Mohammed Ajmal Khan*.

79 As revealed through material presented during the case, on or about July 11, 2000, LeT released an article from the *Taiba Bulletin* online that "quoted an LET official as stating: 'Mujahideen have got access to the Indian army web site where they worked against the Indian forces. Lashkar-e-Taiba also made a remote control aeroplane that was caught in Occupied Kashmir. We are developing the modern technology. We can make modern devices. Alhamdulilah.'" See Indictment, *United States of America vs. Ali Asad Chandia and Mohammed Ajmal Khan*, p. 3.

80 M. A. Khan, "India's RPV Programmes," *Military Technology* (November 1997).

81 Some of the court documents also describe an individual coconspirator who used the name "Pal Singh." This individual was described as another LeT operative who also used the name "Abu Khalid" and "traveled between Pakistan, the United Kingdom, and the United States." Since Khan also used the name Abu Khalid, it appears as though Khan and Pal Singh are the same person, and that "Pal Singh" was another alias used by Khan. See Memorandum Opinion, *United States of America vs. Masoud Khan, et. al*; Indictment, *United States of America vs. Ali Asad Chandia and Mohammed Ajmal Khan*.

82 Ibid.

83 Indictment, *United States of America vs. Ali Asad Chandia and Mohammed Ajmal Khan*.

All three of these individuals were eventually convicted for the roles they played in the conspiracy.[84]

Court records filled by prosecutors in the case reveal that Khan started his dialog with the U.S.-based companies in mid-February 2002, and that his dialog with them continued until at least December of that same year, when some of the purchases were finalized.[85] The e-mails between the parties are revealing, as they highlight the specific technology and associated enhancements that LeT sought, details which provide insight into LeT's likely intended use of the matériel.[86] A lengthy memorandum opinion filed by prosecutors in the case puts these dynamics into context:

> In December 2002, Khan purchased from Vesta Technologies an MP-1000SYS airplane control module. According to the testimony of Cindy Reish, general manager of Vesta Technologies, and the documents regarding the transaction maintained by that company (Ex. 2C2a), the MP-1000SYS is a stability and control computer that can be programmed to fly an airplane with a 10-12 foot wingspan using Global Positioning System ("GPS") coordinates. The unit controls altitude, speed, and navigation to programmed waypoints, and can also be programmed to turn a video camera on and off when the airplane reaches certain locations.
>
> The majority of Vesta's customers for this technology are universities and the government, including NASA and the military. Common applications of the technology are using model airplanes equipped with video devices to monitor forest fires, property boundaries, gas lines, or livestock in remote or inaccessible areas.
>
> Khan first attempted to order the device from Vesta by telephone in December 2002. According to Reish, Khan stressed the urgency of receiving the device before the end of December, and seemed reluctant to fill out paperwork. Reish insisted that Khan fill out the appropriate paperwork, and faxed him an order form on December 11, 2002. Although Vesta is not required to conduct due diligence on domestic purchasers, Reish was suspicious enough of the transaction that she also requested that Khan answer export control questions on the order form. Khan completed the paperwork and faxed it back to Vesta. On the form he listed his address in Gaithersburg, MD and phone number, and indicated that the intended use was "Radio Controlled (RC) model aircraft pilot assist." Other potential uses listed on the form, not selected by Khan, included "Commercial robotic aircraft" and "Military Unmanned Aerial Vehicle." Vesta checked Khan's name against lists of prohibited purchasers for export, and not finding him listed, shipped the device to Khan on December 30, 2002.
>
> Both [Monte] Salot [the president of Wireless Video Cameras] and Reish testified that the wireless video equipment purchased by [Saifullah] Chapman and the airplane control module purchased by Khan are compatible with one another, and that the two types of equipment are commonly used together on model airplanes.…
>
> From this evidence, we draw the inference that Singh's [read: Khan's] procurement of model airplane equipment was for LET's military use in Kashmir. Because Khan [had a]… connection with LET and balked at completing paperwork, we find that Khan was aware and intended that his straw purchase of the autopilot module was for LET'S military use.[87]

Additional details related to the conspiracy are even more revealing, as they outline LeT's interest in not just acquiring the "Radio Controlled model aircraft pilot assist," but also in maximizing the range over which that piece of technology would still work. As noted by Khan in an e-mail that he sent to Vesta Technology on 24 February 2002:

84 See "'Paintball Terrorists' Convicted of Conspiracy," Fox News, March 4, 2004.

85 Indictment, *United States of America vs. Ali Asad Chandia and Mohammed Ajmal Khan*.

86 Ibid.

87 Memorandum Opinion, *United States of America vs. Masoud Khan, et. al*.

> I just got back to DC and read your emaIls, I would like to place the order for complete system however could you find out for me a remote control and video which have greater range. 5 miles+ which is compatible with your system. Please get back to me ASAP so that I could make a final decision. I looked up a video system at www.wirelessvideocameras.com Model AAr05 with TC CMOS This has a range of 5 miles [*sic*].[88]

After receiving a response from Vesta Technology, Khan sent an e-mail with the following details the next day: "Thanks for the quick response I will be waiting for ur info on long range remote controls and any other video systems in regard to ur second email I shall put it to my boss, however I can not garanty [*sic*] anything waiting for info as soon as thanks."[89] Three days later he sent a follow up e-mail to Vesta: "Have you got any news on long range remote transmitters waiting for u [*sic*] reply thanks."[90]

Beginning in May 2002, Khan engaged in a similar dialog with Wireless Video Cameras after he was not satisfied with the performance and range associated with its system.[91] The e-mail correspondence between the two parties illustrates that extending the range of the equipment was a key priority for LeT, as was the reliability of the equipment. Khan's apparent obsession with the range issue one year later even pushed him to seek advice from an Internet site called RCUniverse.com, which provides a forum for its members to ask questions and to crowdsource solutions. In a post he placed on the RC Universe site in May 2003, Khan mentioned, "I have a problem with my RC. I gotta wireless cam capable of sending visual within 4 miles radius, but my RC has the capacity of 2 mile radius, coz my plane gets out of the RC range, I need to enhance the radius of my RC, if anybody has any idea how to boost the range of the TX, that would be appreciated [*sic*]."[92]

HAQQANI NETWORK	2005
Overview: UAS possession; use unclear	

In 2005 a UAS was found at a compound associated with another Pakistan-based organization, the Haqqani network. The UAS was discovered after the Pakistani military conducted a raid on the Haqqani's Manba Uloom madrassa located in Miranshah, North Waziristan.[93] (Some authors have mistakenly identified this episode as an al-Qa`ida case.) As the current author and others have documented, the facility served at the time, and for a period thereafter, as a base friendly to local and foreign militants, including those associated with al-Qa`ida.[94] According to the Pakistani general running a press conference that highlighted the raid, "the terrorists used the [UAS]. . . to check the position of security forces and attack them."[95] Even though details were not provided, the general also added

88 Indictment, *United States of America vs. Ali Asad Chandia and Mohammed Ajmal Khan*.

89 Ibid.

90 Ibid.

91 Ibid.

92 Ibid.

93 For background on the facility, see Vahid Brown and Don Rassler, *Fountainhead of Jihad: The Haqqani Nexus, 1973–2012*, (London: Hurst, 2013), p. 55. Even though there are photos of the UAS available online, press reports conflict regarding what type of UAS it was, as one source says it was a Chinese-made variant, while another report suggests that it was locally made. See "21 Important Tribal Personalities Arrested During Operation in NWA: Safdar," *PakTribune*, September 13, 2005; "Troops Nab Militants, Find Unmanned Drone," *Peninsula Qatar*, September 14, 2005.

94 For additional background on the incident, see Behroz Khan, "5,000 More Troops Sent to Pak-Afghan border," *The News*, September 14, 2005; Iqbal Khattak, "40 Militants Killed in North Waziristan," *Daily Times*, 30 September 2005; "Pakistani Law Enforcers Intensify Hunt for Haqqani," *Pajhwok Afghan News*, March 7, 2006.

95 "Troops Nab Militants, Find Unmanned Drone."

that "the drone was capable of carrying weapons."[96] Besides this incident, the author was not able to find evidence of the Haqqani network or al-Qa`ida in the Afghanistan-Pakistan region using a UAS in the field. That being said, the Haqqani network, and particularly the group's founder, Jalaluddin Haqqani, has long had a penchant for innovation, so the group's future use of this type of platform in that region seems likely.

Material recovered during a raid on Haqqani network facility, 2005 (Getty Images)

CHRISTOPHER PAUL	2006
Overview: Research on UAS only; formal tie between suspect and al-Qa`ida	

The next case is one that many analysts have labeled as a UAS-affiliated plot, and one with ties to al-Qa`ida. The case involves Christopher Paul (also known as Paul Kenyatta Laws or Abdulmalek Kenyatta), a U.S. citizen and a seasoned jihadi operative with personal ties to al-Qa`ida that reach back as far as the early 1990s.[97] After training with al-Qa`ida in Afghanistan, Paul conducted jihad in Bosnia.[98] According to the three-count indictment filed against him in the United States in 2007, in addition to providing material support to a terrorist entity and attempting to use a weapon of mass destruction (WMD) against a U.S. national abroad, Paul also interacted with and supported a number of terrorist cells in Europe.[99] The indictment also claims that in 2006 Paul conducted research on the use of remote-control devices, specifically "remote controlled boats and a remote-controlled 5-foot long helicopter."[100] In a plea deal struck in 2008, Paul pled guilty to the WMD charge, and the other charges were dropped.[101] Thus, while there is evidence that Paul had an interest in UAS technology,

96 Ibid.

97 For background, see "Ohio Man Pleads Guilty to Conspiracy to Bomb Targets in Europe and the United States," Department of Justice, June 3, 2008.

98 Indictment, *United States of America vs. Christopher Paul*, April 7, 2011; Plea, *United States of America vs. Christopher Paul*, June 2, 2008; Judgment, *United States of America vs. Christopher Paul*, February 26, 2009.

99 Ibid.

100 Indictment, *United States of America vs. Christopher Paul*.

101 Plea, *United States of America vs. Christopher Paul*.

there is not enough evidence to indicate that his interest in UASs reached beyond curiosity to the level of a bona fide UAS terror plot.

EGYPT PLOT	2008
Overview: Purchase of UAS controller; alleged ties to HAMAS	

A case that is even less clear took place in Egypt in 2008. According to two press reports, in 2008 Egypt charged five individuals, "two leaders of the opposition Muslim Brotherhood, two Sinai Bedouins and a Palestinian[,] with plotting a terrorist attack with Hamas."[102] The reports claimed that the two Muslim Brotherhood leaders, Abdel-Hai al-Faramawy and Mohammed Wahdan, purchased "30 jerry cans of fuel, spare parts and a remote control for an unmanned aircraft" from the two Sinai residents, and did so with the intent to provide the material to HAMAS, which allegedly wanted to use the material to help build a UAS to strike at an unknown target.[103] The two brothers and HAMAS denied the charges, and the author could not find information regarding how this case was resolved; specifically, the author could not determine whether the five individuals were convicted or if the case was dismissed.[104] Thus, without additional information, this case can only loosely be understood as a credible UAS terror plot.

REZWAN FERDAUS	2011
Overview: Purchase and testing of UAS; attempt to weaponize UAS for attack	

The most noteworthy domestic UAS plot is the one involving Rezwan Ferdaus, a U.S. citizen in his midtwenties who studied physics at Northeastern University.[105] The treatment of Ferdaus's case in the media varies widely, as while some have used his case to highlight and call attention to the serious nature of the threat posed by terror-linked UAS plots, others have used his case to argue just the opposite, that the terrorist threat from UASs is inflated.

The primary strategic flaw associated with Ferdaus's plot was the major disconnect that existed between his grand vision for the operation and the project's feasibility. This issue is compounded by the fact that Ferdaus was naive enough to become ensnared in a FBI sting operation, and that some of the changes Ferdaus made to his plan, which actually would have enhanced the plot's feasibility, occurred after his dialogue with the FBI's cooperating witness (CW) had started.

When the FBI's CW initially discussed the attack ideas with Ferdaus in early 2011 the latter's plan was to use a GPS-guided and explosive-filled UAS to attack the Pentagon.[106] At the time, Ferdaus claimed that he had the "knowledge of GPS and electronics and the skills to make it happen" and that he

102 Pakinam Amer, "Egypt Charges 5 with Plotting an Attack with Hamas," Associated Press, April 27, 2008; "Internet Post Discussed Unmanned Plane Attacks, Egypt Says It 'Foiled Aerial Drones' Plot," CBS News, April 28, 2008.

103 Ibid.

104 Ibid.

105 For background on Rezwan Ferdaus, see Peter Finn, "Mass. Man Accused of Plotting to Hit Pentagon and Capitol with Drone Aircraft," *Washington Post*, September 28, 2011.

106 Decision on the Government's Motion for Detention, *United States vs. Rezwan Ferdaus*, November 28, 2011.

wanted to "recruit some 'brothers'… [who] would have to be prepared spiritually to die."[107] The CW led Ferdaus to believe that through him he would be in contact with al-Qa`ida and that he and two undercover FBI agents who were pretending to be al-Qa`ida members would be providing Ferdaus with opportunities to illustrate his commitment to the effort and to further develop and carry out his plot.[108]

To support his vision, Ferdaus asked the CW to acquire "enough explosive material to take out a target that is about three football fields long."[109] Excited that his initial plan would come to fruition, a week or so later Ferdaus mentioned that he was also considering the United States Capitol, politicians, a subway station, and a military facility in Colorado as other potential targets.[110] After some deliberation, Ferdaus ultimately settled on a plot involving three drones filled with explosives that would attack the Pentagon and the U.S. Capitol.[111] One of those drones would be flown into the Capitol dome, as Ferdaus believed that such a strike would cause the dome to collapse.[112] The other two drones would be "flown into opposite sides of the Pentagon" to facilitate destruction and the funneling of Pentagon workers out of the building, where they would be picked off by the armed "brothers" Ferdaus wanted to have lying in wait.[113]

The remote-control "planes he chose were small replicas of F-4 Phantoms and F-86 Sabre jets, each plane being around "5 to 7½ feet long guided by GPS devices and capable of speeds over 100 mph."[114] Ferdaus initially envisioned that each UAS would "be filled with 16 grenades" and that the attack on the Pentagon would have such a profound impact that it would "essentially decapitate the entire empire… [and] severely disrupt the head and heart of the snake" (phraseology that al-Qa`ida uses to refer to the United States).[115] Realizing that his plan to use grenades was perhaps more complicated than it needed to be (see later in this subsection), he asked the FBI informant to acquire enough of the military-grade explosive C-4 to "place 5 pounds of C-4…within each of the replica jets."[116]

One thing that is not in dispute is Ferdaus's intent to carry out his plan, as the actions he took and believed to be inflicting harm on U.S. armed forces personnel were real. For example, to "vet" Ferdaus as an operative, the FBI (acting as al-Qa`ida) asked him to develop of number of improvised explosive device triggers that the group could use to "kill American soldiers stationed overseas."[117] As noted by the criminal complaint filed in his case, Ferdaus "designed, built and supplied more than 7 mobile phones, each of which Ferdaus had modified to act as an electrical switch for an improvised explosive device… to FBI undercover employees."[118] As John Mueller has noted, the "court deemed Ferdaus to be a "a significant danger to the community," not because his plot would have worked or because he had the means to carry it out, but, as Mueller's report emphasized in italics, because he had a "*strong desire to see his plan carried out.*"[119]

---

107 Ibid.

108 For detailed background see Affidavit, *United States vs. Rezwan Ferdaus*, September 28, 2011.

109 Decision on the Government's Motion for Detention, *United States vs. Rezwan Ferdaus*, November 28, 2011.

110 Criminal Complaint.

111 For background, see Decision on the Government's Motion for Detention, *United States vs. Rezwan Ferdaus*, November 28, 2011.

112 Affidavit, *United States vs. Rezwan Ferdaus*, September 28, 2011.

113 Decision on the Government's Motion for Detention, *United States vs. Rezwan Ferdaus*, November 28, 2011; Criminal Complaint; Affidavit, *United States vs. Rezwan Ferdaus*, September 28, 2011.

114 John Mueller, "Case 46: Model Planes," in John Mueller, ed., *Terrorism Since 9/11: The American Cases* (Washington, D.C.: Cato Institute, March 16, 2014), p.5.

115 Affidavit, *United States vs. Rezwan Ferdaus*, September 28, 2011.

116 Mueller, "Case 46," p. 6.

117 Affidavit, *United States vs. Rezwan Ferdaus*, September 28, 2011.

118 Ibid.

119 Mueller, "Case 46," p. 1.

Ferdaus's plot certainly faced a number of technical hurdles. First, to get his drones into the air, Ferdaus would "have needed a pretty long runway."[120] According to his charge sheet, Ferdaus surveyed and intended to use East Potomac Park for that exact purpose.[121] A second significant hurdle was the issue of UAS payload limitations. There were also doubts about the UAS's flight stability, which would have made controlling the UASs problematic and decreased their ability to deliver their payloads to the intended targets. In an interview with CBS News, Greg Hahn, the technical director of the Academy of Model Aeronautics, noted that "the idea of pushing a button and this thing diving into the Pentagon is kind of a joke, actually."[122] Hahn went on to add that "the heavier of the two [UAS] models Ferdaus was allegedly planning to use could carry a maximum of two pounds of plastic explosives before malfunctioning. That's not including the weight of any GPS system."[123] As noted earlier in this subsection, Ferdaus wanted to load each of the UASs with five pounds of C-4, suggesting that he would have faced problems accurately controlling the machines. The "added weight would throw them off balance and make them uncontrollable, a key defect in that, to do any serious damage, they would have to be flown into windows, and at high speed."[124]

A third hurdle was the issue of detonation. Ferdaus's initial thinking on this topic only further confirms that even though some of his ideas were amateurish and unsophisticated, he wanted to see his plot through. For example, before he requested C-4 from his purported al-Qa`ida handlers, Ferdaus wanted to place grenades in each of the drones, and to detonate them with a "high-torque servo motor" that would pull the pins from the grenades at the appropriate time in flight.[125] Experts suggest that this is a complicated task. As noted by James Crippin, an explosives expert, even "getting a stable explosive like C-4," which Ferdaus requested, "to blow up at the right time [and place] would have been hugely difficult."[126] Further, as Crippin went on to add, "there were slim prospects of causing any serious damage to buildings like the Pentagon and Capitol, which are undoubtedly hardened to withstand explosions.… Basically, I think he's suffering from delusions of grandeur."[127]

At the conclusion of his case, Ferdaus received a sentence of seventeen years in prison, with a decade of supervised release.[128] As his conviction and sentencing illustrate, none of this is to suggest that Ferdaus wasn't dangerous, or that, left unfound, he wouldn't have found a way to see his plan through to fruition, however amateurish or lackluster it may have been. The danger of the Ferdaus case lies less with Ferdaus as an individual and his apparent lack of sophistication, and more in the precedent he and his case set: specifically, how a domestic extremist with violent intent who was motivated by al-Qa`ida identified a UAS as his preferred attack platform, more than five years ago.

120 Adam Weinstein, "A Terror Plot Wile E. Coyote Might Love," *Mother Jones*, September 30, 2011.

121 Affidavit, *United States vs. Rezwan Ferdaus*, September 28, 2011.

122 "Could Model Airplanes become a Terrorist Weapon," CBS News, September 29, 2011, as cited in Mueller, "Case 46," p. 7.

123 Ibid.

124 Ibid.

125 Ibid., p. 6.

126 Ibid.

127 Ibid.

128 U.S. Attorney's Office, District of Massachusetts, "Man Sentenced in Boston for Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Detonation Devices to Terrorists," November 1, 2012.

Two UASs associated with Rezwan Ferdaus's plot (2011) (U.S. Department of Justice)

GIBRALTAR CLIQUE	2012
Overview: Purchase and testing of UAS; suggested ties between suspects and al-Qa`ida	

The story of Cengiz Yalcin, a Turkish citizen, and two Chechens, Mohammed Ankari Adamov and Eldar Magomedov, provides a glimpse into how the initial media response to a suspected UAS-linked terror plot can take on a life of its own. In August 2012, Spanish authorities arrested these three individuals on charges stemming from their alleged plans to attack a shopping center in Gibraltar using either a UAS or manned paragliders, or both, for an attack that was to coincide with the 2012 London Olympics.[129] Spanish authorities were concerned about the trio because of their alleged associations with al-Qa`ida. During a training flight with one of their paragliding instructors, one of these individuals "asked his instructor about taking photographs of Gibraltar shopping centre from the air."[130] In a press conference after their arrest, Jorge Fernández Díaz, the Spanish minister of the interior, described the trio as "extremely dangerous people," with one of the men being a "very important operative in al-Qaeda's international structure."[131]

After the Spanish police raided Yalcin's home, they found traces of explosives in his garage.[132] The police also found a video that showed "a test [flight] with a model aircraft . . . with a wingspan of 2 meters and the capacity to carry up to 1 kg of explosives" that Yalcin and another person had made.[133] The investigators claimed that this video provided proof that the trio was planning to use the UAS "to release a device," likely an explosive one.[134] The problem, as noted by David Eade, a journalist who wrote a follow-up piece about the case in 2014, was that "neither Yalcin nor the other two were ever brought to trial for these offences."[135] Further, on "the 10th April 2013 they were all freed as there was no proof against them. The explosives seemingly never existed. The Chechens were deported. Yalcin, although a Turkish national, still lives openly at his La Línea home."[136]

129 For background, see "Spain Charges Two Russian Citizens in al-Qaeda Terror Plot," RT, August 5, 2012; "This Is How the Detained Al-Qa'ida Terrorists Were Testing an Aerial Attack in Cadiz," *El Pais*, August 11, 2012; Karl Smallman, "Gibraltar 'Terror Trio' Released," *Olive Press*, April 2, 2013.

130 Smallman, "Gibraltar 'Terror Trio' Released."

131 "Spain Charges Two Russian Citizens in al-Qaeda Terror Plot."

132 David Eade, "Islamic Terrorist or Innocent Man," *London Progressive Journal*, February 15, 2014.

133 "This Is How the Detained Al-Qa'ida Terrorists Were Testing an Aerial Attack in Cadiz."

134 Ibid.

135 Eade, "Islamic Terrorist or Innocent Man."

136 Ibid.

Video of UAS taken from Yalcin's apartment. (Spanish Interior Ministry; Al-Arabiya)[137]

This case thus illustrates only UAS interest by a small group that is suspected, and not proven, to have been acting on behalf of al-Qa`ida and with terror intent.

GERMAN PLOTS	2013
Overview (**Tunisian students**)**:** Alleged desire to weaponize a UAS **Overview** (**Right-wing extremists**)**:** Possession of UAS and bomb material; plans to weaponize	

In the summer of 2013, German authorities reportedly disrupted two separate cells that were planning to use drones to conduct terror attacks. The first group involved a group of "Tunisian aeronautic students in Stuttgart, Munich, and Dachau" who were reportedly "developing missile-carrying drones" that they wanted to use as part of an operation.[138] Then, that same summer, German police disrupted a cell of right-wing extremists who appear to have had a similar intent.[139] During the raid on a compound that was being used by that second group, the German police "recovered bomb-making materials and a drone," stating later that the cell was "allegedly planning to use the device to bomb a German summer camp."[140] It is not clear, given this group's intended target, if it wanted to emulate or was inspired by the actions of the convicted right-wing Norwegian terrorist Anders Breivik, who in 2011 killed close to seventy young people after he attacked a summer camp for youth close to Oslo.

FATHI CASE	2014
Overview: Interest in UAS as an attack platform	

A number of analysts and reports have also included the 2014 case of El Mehdi Semlali Fathi as addi-

137 Eman el-Shenawi, "Toy Planes and Miniature Bombs: How al-Qaeda Plots Terror," *Al-Arabiya*, August 14, 2012.

138 For background, see "Two Men Investigated in Germany over Alleged Terror Plot Using Model Planes," *Daily Mirror*, June 25, 2013; Jean-Paul Ney, "Terrorist Drones: States Are Taking Steps," Infosdefense.com, October 15, 2013. There is a discrepancy between these two sources, as one mentions that the Tunisian students were investigated, while another says they were arrested.

139 Jack Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns," *Wall Street Journal*, January 29, 2015.

140 Ibid.

tional evidence of the rising terrorist use of UASs. The problem, as the writer Sean Lawson has pointed out, is that "this case of supposed 'drone terrorism' has been greatly exaggerated."[141] As Lawson notes:

> The affidavit… filed in Mr. Fathi's case indicates that in January 2014 he came under federal investigation as a result of statements indicating his aspirations to carry out bomb attacks against Harvard University and a federal building in Connecticut where he lived. The affidavit stated that in recorded conversations, Fathi had expressed his aspiration to use what the federal agent called "toy planes" or "a remote-controlled hobby-type airplane, to deliver the bomb."[142]

So the initial impetus that drove the FBI's investigation were the threatening statements that Fathi made about his desire and alleged plan to attack those two facilities. At least in his eyes, a UAS was the attack platform that he would have wanted to use in this future, aspirational attack. The problem, again as noted by Lawson, was that after learning of Fathi's vision:

> The government did not wait to find out whether Fathi truly intended to or was capable of carrying out these attacks. During the course of the investigation, they learned that Fathi had lied on his application for refugee status and in statements to multiple immigration judges. The government therefore sought a warrant for Fathi's arrest on three counts: making false statements, false swearing in an immigration matter, and perjury. Fathi was only charged… with one of those, perjury. In short, though statements about bombing with "toy airplanes" may have been the impetus for the initial investigation, he was neither arrested for, nor charged with, making terrorist threats.[143]

This isn't to say that left to his devices, Fathi would not have acted on his vision and transformed his aspirations to conduct an attack using a UAS into an actual, concrete plan. It just isn't clear that Fathi had the skills, will, know-how, or sophistication to execute such a plot. Therefore, this UAS plot is best understood as being one that was aspirational only, and one that was based entirely on the subject's interest in drones as a technology and a potential weapons delivery platform. In that regard, given how many media outlets were quick to run with and frame the Fathi story as being one that was a substantive UAS plot, it offers a cautionary tale about, as Lawson puts it, the "fear-induced technopanic and threat inflation related to domestic drones."[144]

TURKISTAN ISLAMIC PARTY	2016
Overview: Strategic communications	

In 2016, the Syria faction of the Turkistan Islamic Party used drones to film two separate incidents. In April of that year, the group used a drone to film a large vehicle-borne improvised explosive device (VBIED) attack in Syria.[145] Several months later, in August, the group leveraged a UAS to document fighting in the Syrian town of Aleppo.[146] The footage from both incidents was repackaged and incorporated into propaganda videos that the group posted online.

141 Sean Lawson, "The Drone Terrorism Case that Wasn't," *Forbes*, December 8, 2014.

142 Ibid.

143 Lawson, "The Drone Terrorism Case that Wasn't"; for additional background, see Alex Brandon, "FBI: Man Plotted to Fly Drone-Like Toy Planes with Bombs into School," Associated Press, April 8, 2014.

144 Ibid.

145 Twitter post by @thomasjoscelyn, April 22, 2016.

146 Twitter post by @thomasjoscelyn, August 19, 2016.

Groups with UAS Programs

HEZBOLLAH	First sign of program: 1997
UAS Use: surveillance, external communications, weaponization	
Takeaways: Key UAS innovator; UAS weaponized; typically uses modified Iranian UAS variants	

The terror group with the most sophisticated and long-standing UAS program is Hezbollah.[147] The genesis of Hezbollah's program can be traced back to at least 1997, when Hezbollah operatives in southern Lebanon were able to gain access to Israeli UAS feeds.[148] This allowed the group to monitor the Israeli feeds and to gain useful intelligence on the locations that the Israeli military was monitoring across its border in Lebanon, including the infiltration route that a team of Israel's elite Shayetet 13 naval commandos would later use during a sensitive operation.[149] According to a number of sources, the monitoring was relatively easy for Hezbollah to do at the time because the Israeli UAS feeds used by Shayetet 13 were either unencrypted or not encrypted well.[150] Some sources even suggest that glimpses of these feeds could be seen openly on local television channels.[151] Other sources suggest that a double agent who was working for but later turned on the Israelis played a role as well.[152] Not knowing that Hezbollah was monitoring its feeds and potentially aware of insider information, Israel sent a small assault force in September 1997 to conduct a secret, surprise raid into Lebanon to target a Hezbollah leader. When they did, the force was confronted by mines and a well-prepared team of operatives who were ready for them.[153] The Israeli team was ambushed and the operation ended in disaster, resulting in the death of at least eleven Shayetet soldiers and a doctor accompanying them.[154] In its analysis of the episode, which was dubbed the "Ansariya ambush" in the Israeli media, Hezbollah likely realized two things: (1) that even though it had been able to outsmart the Israelis on this occasion, UASs were still a threat; and (2) that UASs were a tool that it wanted for its own purposes.

The individual who helped Hezbollah with the technical aspects of intercepting the Israeli feeds in 1997 was Hassan al-Lakkis, described as being one of Hezbollah's "brightest minds," who would serve as the group's chief procurement officer and later play "a key role in developing Hezbollah's unmanned aerial vehicles program."[155] Hassan al-Lakkis's importance to Hezbollah is reflected by the fact that he was the target of several Israeli assassination attempts, and that after he was successfully killed by Israel in December 2013, "the top brass of Iran's elite Revolutionary Guard attended… [his funeral],

147 The author acknowledges that there is a debate about whether Hezbollah is only a terror organization, and he recognizes that Hezbollah is a complex organization whose activities (i.e., political and social) extend well beyond those traditionally pursued by terrorist groups and that Hezbollah is best understood as being a hybrid political-terrorist entity. The author has decided to include Hezbollah under the terrorist group label because it remains designated as a Foreign Terrorist Organization by the U.S. government.

148 To see Hezbollah's treatment of this issue, see www.youtube.com/watch?v=ivvMuKhF6x4.

149 Batsheva Sobelman, "Hezbollah News Conference Brings Truth on Botched Lebanon Raid," Babylon and Beyond Blog, November 7, 2010; Yaakov Katz, "Israel Air Force Initiates Drive to Encrypt All of Its UAVs," *Jane's Defence Weekly*, November 26, 2010.

150 According to one source, only the UAS feeds of Israeli's Sayeret Maytal unit were encrypted at the time. See Sobelman, "Hezbollah News Conference Brings Truth on Botched Lebanon Raid."

151 Ibid.

152 Robert Fisk, "Israel Ambushed: Double Agent Lured Soldiers to Death in Lebanon," *Telegraph*, September 16, 1997.

153 Sobelman, "Hezbollah News Conference Brings Truth on Botched Lebanon Raid."

154 Ibid.

155 "Hezbollah Vows Israel Will Pay for Lakkis' Killing," *Daily Star*, December 20, 2013; Ali Hashem, "Assassinated Hezbollah Leader Key to Technology, Drone Operations," *al-Monitor*, December 4, 2013; Matthew Levitt, *Hezbollah: The Global Footprint of Lebanon's Party of God* (Washington, D.C.: Georgetown University Press, 2013), pp. 166–68.

including the commanders of the Quds Force, [and the] navy, air and land forces."[156] Hezbollah also vowed that his death would be avenged.[157]

While open-source records do not reveal a precise start date for Hezbollah's program, the formal elements of the group's program are highly likely to have started shortly after the Ansariya ambush. According to an Israeli intelligence source interviewed by RAND, Hezbollah had already "begun to experiment with unmanned aerial vehicles" shortly thereafter the "time of the al-Aqsa Intifada" (2000–2005).[158]

Since its inception, Hezbollah has benefited from its close relationship with the Iranian state, and many of the drones that Hezbollah has flown over the last decade are believed to be modified variants of domestic UASs that Iran has developed for military purposes. A number of Iranian government officials have openly acknowledged that the Iranian government has shared UAS technology with its partner Hezbollah.[159] It is believed that the roots of Iran's own UAS program date back to the Iran-Iraq War, which is a factor that helps explain, given the historical relationship between Hezbollah and Iran, why Hezbollah's drone program is more sophisticated than those of other terror entities'.[160] Iran, and by extension Hezbollah, has simply been in the UAS game longer than other groups.

In 2004 Hezbollah and its UAS program took a major step, as in November of that year the group flew a UAS from southern Lebanon across the Israeli border. The UAS reportedly "passed over the northern Israeli town of Nahariya, and then turned west and returned to Lebanese territory, landing in the Mediterranean Sea not far from shore."[161] During this UAS flight, Hezbollah was able to fly the device over Israeli airspace for between fifteen and thirty minutes.[162] Although the device is reported to have been undetected by Israeli radar, it was "noticed by local residents" who said that the UAS was noisy.[163] It is believed that the UAS, which Hezbollah named the Mirsad-1, was either a variant of the Mohajer-4 or Ababil-T drones, both produced by Iran.[164] Hezbollah "released a grainy twenty-second video of the flight" the next day, "claiming that the aircraft could fly 'deep, deep' into Israel."[165] The flight was certainly a public relations win for the group. It was also an early indicator of a wave of additional UAS flights to come.

156 "Revolutionary Guard Leaders Pay Tribute to Slain Lakkis," *Daily Star*, January 9, 2014.

157 Dana Kraiche, "Hezbollah Vows Israel to Pay for Lakkis Killing," *Daily Star*, December 30, 2013.

158 This data point is sourced to interviews RAND conducted with security officials in Israel; see Kim Cragin et al., *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies* (Santa Monica, CA: RAND Corporation, 2007), p. 52.

159 "Profile of Hezbollah," *Jane's*.

160 Gettinger et al., *Drone Primer*, p. 8; for background on Iran's drone arsenal, see Arthur Holland Michel, "Iran's Many Drones," Center for the Study of the Drone, November 25, 2013; see also Adam Rawnsley, "Syria's 'New' Iranian Drone," Bellingcat, January 28, 2016.

161 "Primary Sources," *Atlantic*, March 2005.

162 Ibid.

163 Ibid.

164 "Profile of Hezbollah," *Jane's*.

165 "Primary Sources."

Photo Credit: Screen grabs from al-Manar video rereleased by the Associated Press[166]

Less than six months later, in April 2005, Hezbollah flew another UAS into Israel.[167] The launch of that UAS was followed by a speech released by Hassan Nasrallah, the group's secretary general, in which he claimed that Hezbollah's drones could be "packed with 40–50 kg of explosives" and be used "to attack priority targets deep inside Israel."[168] While Hezbollah had clearly developed an important capability, Nasrallah's claims about the load-bearing capability of his group's drones had not been publically verified. Yet they were still a threat that the Israeli military was taking very seriously.[169]

The next year, 2006, was also an important year for the Lebanese group's UAS program. During its war with Israel that year, Hezbollah launched at least three drones into Israeli airspace. All three of these drones were reportedly shot down in flight by the Israeli Defense Forces (IDF).[170] According to Paul Burke and a number of other sources, "one of these UAVs was loaded with around 30 kg of explosives and was intended to be used as a guided bomb, effectively a cruder version of a cruise missile. The remains of the payload-configured UAV were discovered close to Nahariya, near Haifa."[171] As Burke noted, the discovery by the IDF was significant, as it represented the first successful attempt by a terrorist group to load a conventional weapon onto a UAS.[172] Even though these UAS flights, and the ones flown prior, were not able to cause devastation, they were still a success for Hezbollah, as they likely helped the group instill fear in its enemy Israel and rally support back home.

In 2010 Israel again faced problems with the encryption of its UAS feeds. Israel's government realized this was an issue after Hassan Nasrallah "revealed footage from what he claimed was [an] Israel Aerospace Industries (IAI) Searcher Mk II multimission tactical UAV that had conducted surveillance over an orchard raided by Israeli commandos,"[173] Israel set up a commission to investigate the claim, which it was eventually able to corroborate.[174] This led to a decision by the Israeli air force to "encrypt its entire fleet of unmanned aerial vehicles to prevent Hizbullah and HAMAS from intercepting" its feeds.[175] The incident also reinforced the cat-and-mouse dynamic that is at play between Israel and its primary nonstate-actor adversaries when it comes to UASs and the technology they have on board.

166 See www.youtube.com/watch?v=ONwb5_VtQbY.

167 "Profile of Hezbollah," *Jane's*.

168 "Israel Intercept Two Attack UAV Launched by Hezbollah," Defense Update, August 14, 2006,.

169 For background, see Arie Egozi, "Hostile UAV Threat Alarms Israel," *Flight International*, November 16-22, 2004.

170 Paul Burke, "The Terrorist Threat to the Maritime Security of the UAE," Emirates Center for Strategic Studies and Research, Emirates Lecture Series No. 85, 2010.

171 Ibid.

172 Ibid. It is still not clear if the attempt by Aum Shinrikyo should be considered the first attempt to weaponize a UAS, even though the group potentially weaponized its remote-control helicopter with unconventional weapons. There is a need for additional information to firmly establish this point.

173 Yaakov Katz, "Israel Air Force Initiates Drive to Encrypt All of Its UAVs," *Jane's Defence Weekly*, November 26, 2010.

174 Ibid.

175 Ibid.

Hezbollah's UAS flights into Israel continued over the next several years. In October 2012, Hezbollah flew a modified Iranian UAS deep into Israeli airspace "over sensitive and important locations" before the aircraft was downed.[176] According to some reports, the UAS conducted reconnaissance of "preparations for Israel's biggest joint military exercise with the US Army… as well as ballistic missile sites… [and] main airfields."[177] In a video released by Hezbollah's al-Manar television station, Hassan Nasrallah also claimed that the UAS overflew Israel's Dimona nuclear facility, "one of the most protected sites in the whole country."[178] Other sources indicate that the UAS was only headed in the direction of Dimona, and that Hezbollah was not able to overfly the sensitive site.[179]

Hezbollah flew another UAS into Israel in April the following year.[180] That aircraft was also downed by the Israeli military.[181] Then in September 2014, Hezbollah claimed to have hit another major milestone: the firing of a missile from one of its UAS platforms. The group claims that during a flight near Arsal, Lebanon, one of its UASs successfully fired an armed missile that reportedly killed over twenty members of Jabhat Fateh al-Sham that were operating in Syria.[182] Even though Hezbollah's use of UASs in Syria has been well established, Hezbollah's hitting this milestone has been "corroborated" only by Iranian media outlets, which has done little to bolster the group's claim.[183]

The discovery in April 2015 of what is believed to be a Hezbollah UAS airstrip in Lebanon's Bekaa Valley (satellite pictures of which are available online) and the group's more recent use of commercially available UASs to augment its operations and larger military-grade drone fleet indicate that Hezbollah's UAS program continues to develop and is here to stay.[184]

176 Anne Barnard, "Hezbollah Says It Flew Iranian-Designed Drone into Israel," *New York Times*, October 11, 2012; Uzi Mahnaimi, "Security Shambles as Hezbollah Drone Spies on Israeli Army," *Times Online*, October 14, 2012.

177 Uzi Mahnaimi, "Security Shambles As Hezbollah Drone Spies on Israeli Army," *Times Online*, October 14, 2012.

178 Ibid.; "What You Need to Know about the Escalating Drone War in Israel," *New Republic*, July 14, 2014; for Hassan Nasrallah's original video, see www.youtube.com/watch?v=bGc_4M0iCWw.

179 "What You Need to Know about the Escalating Drone War in Israel."

180 Avi Issacharoff, "PA Forces Thwart Hamas Attack Drone Plot in West Bank," *Times of Israel*, October 25, 2013.

181 Gili Kohen, "HAMAS Has More Drones Up Its Sleeve, Defense Officials Say," *Haaretz*, July 14, 2014.

182 Adiv Sterman, "Hezbollah Drones Wreak Havoc on Syrian Rebel Bases," *Times of Israel*, September 21, 2014; Abbott et al., "Hostile Drones."

183 A video that shows the alleged strike was also released, although it is not clear how authentic the video is, or what exactly the video shows. See www.youtube.com/watch?v=uYaHhr5A8rE.

184 Abbott et al., "Hostile Drones;" Friese et al., "Emerging Unmanned Threats," p. 46. For an example of how Hezbollah has used UASs to augment conventional operations, see, as cited by Friese, Nicholas Blanford, "Hezbollah Acquiring New Tactics in Syria," *Daily Star*, May 29, 2015.

Photo Credit: Jane's/Google Earth

Indeed, a short video that appeared online in early August 2016, which reportedly shows Hezbollah dropping two cluster bomblets from a modified commercial UAS onto a rebel position in Syria, demonstrates how the group continues to serve as a leader in the terror UAS use space.[185] Statements made by Hezbollah's leaders also indicate that the group is developing plans to use UASs in unique and new ways, such as crashing kamikaze drones into helicopters.[186] Based on its history, Hezbollah's activity will certainly be a leading indicator, and it will remain a key group to watch.

HAMAS	First sign of program: 2003
UAS Use: Surveillance, external communications, alleged weaponization	
Takeaways: Program lags behind Hezbollah's; UASs not as capable	

Hezbollah has long served as a strategic partner to the Palestinian terror group HAMAS, and that relationship extends to the technology sphere.[187] HAMAS's UAS efforts and use of associated technology usually lag behind those first exhibited by the Shi`a militant group. Thus, analysts looking to predict future HAMAS UAS capabilities and tactics, and techniques and procedures, should look to Hezbollah and its own developments for guidance.

The year 2003 was an important one for information about HAMAS's UAS efforts, and those of other linked Palestinian groups. In January, a news website called DEBKAFile that reports on Israeli military and intelligence affairs claimed, based on anonymous counterterrorism sources, that Fatah had purchased a significant quantity of remote-control toy planes from Europe, and that the group planned to them load with explosives so they could be used for an attack.[188] To this author's knowledge, this report has never been corroborated, and some reports on historical UAS use have accepted this single-source account without questioning its veracity. They have also not tied this incident to other, similar reports filed during the same period.

185 Kyle Mizokami, "Terrorist Group Hezbollah Is Reportedly Using Drone Bombers," *Popular Mechanics*, August 16, 2016; for a link to the video posted online, see www.youtube.com/watch?v=MLnRt9CZz58.

186 Michael Rubin, "Iran's Army to Use Suicide Drones," American Enterprise Institute, April 2, 2015.

187 Cragin et al., *Sharing the Dragon's Teeth*.

188 "Arafat's New Terror Weapon: Exploding Toy Planes," *Debka Files*, January 14, 2003.

For example, three days after the original DEBKAFile story, the Israeli newspaper *Ma'ariv* released an article that made a similar claim.[189] But this time concern centered on HAMAS and not Fatah. According to the author of the piece, Amit Cohen, "for almost six months, HAMAS people have been holding intensive discussions on the movement's Internet sites about developing a new weapon: Model airplane bombs."[190] Cohen went on to share a post from one of the unidentified HAMAS sites that he had been monitoring.

> Subject: Building a model airplane
>
> In the name of Allah, the Compassionate, the Merciful,
>
> In order to build a model airplane, all we need is simple equipment, as follows:
>
> 1. Long-range, remote radio control, receiver, transmitter (as in toy cars, but stronger).
>
> 2. The body of the model should be made of wood, and it is important that it should be light-weight.
>
> 3. Electric or diesel engine. There are small, single-cylinder diesel engines.
>
> 4. A small number of engines ('servo' engines) to control the wings and the other mechanical parts.
>
> 5. Electric battery, petrol tank, and storage area (for explosives…).
>
> A small, basic model plane as described can carry a small quantity of explosive. The building of a large model plane, which can carry a serious quantity of explosive, is a more complicated matter. Such a plane can vary from 40 centimeters to 1.5 meters in size.
>
> I shall try and obtain photos that will show how it is possible to equip such a plane with explosives and intelligence equipment. Regards.[191]

According to Amit, the HAMAS supporters he was monitoring also went back and forth online about some of the limitations of drones. Two key areas of discussion were the payload limitations of model planes (and their need for sizable, and thus identifiable runways) and the problems associated with the range and control of such an aircraft at longer stand-off distances.[192] To get around the first problem, the supporters suggested that HAMAS should consider using remote-control helicopters instead of planes, due to a helicopter's ability to take off from almost any location.[193] "To overcome" the second problem, "a Hamas supporter, an electronics engineer from Saudi Arabia, suggested" and allegedly provided a drawing that showed how the plane could be controlled by a cell phone, which he claimed would extend the range.[194] Other users chimed in that the latter solution was not an easy thing to do.[195]

The following month, in February 2003, in potential confirmation of this account, an Israeli television channel reported that it had received a HAMAS leaflet claiming that the IDF had conducted a strike that killed six of its men.[196] According to the news report, the HAMAS statement claimed that the six

189 Amit Cohen, "Hamas' Air Force," *Ma'ariv* (in Hebrew), January 17, 2003, pp. 18–19.

190 Ibid.

191 Ibid.

192 Ibid.

193 Ibid.

194 Ibid.

195 Ibid.

196 "Sulayman al-Shafi Report from Gaza," Channel 2 Television (in Hebrew), February 16, 2003.

men who were killed "were busy assembling an unmanned aerial vehicle."[197] These reports, and another filed in November of that same year, which raised concerns about the theft of an Israeli UAV from a local UAS manufacturer that some believed might have been sold to local terrorists, illustrated that the potential use of a UAS by terrorist outfits was evolving into a multigroup problem, and broader strategic issue, for the Israelis.[198]

For example, by 2005 Israel's security forces had concerns that UAS would also be used by radical right-wing Jewish extremist groups. They were particularly concerned about Jewish extremists using an explosives-laden UAS (or rockets) to attack the Temple Mount, a major religious site in Jerusalem that houses the al-Aqsa Mosque and the Dome of the Rock, and is important to both Muslims and Jews.[199] During that same year, Israeli intelligence services broke up a cell that was attempting to transfer UAS technology and know-how from a company in the United Arab Emirates to HAMAS. According to an Israeli article about the incident, the "man who spearheaded the group was Ibrahim Sawalha."[200] Sawalha was a mechanical engineer from the West Bank who reportedly found "work at a company [in the United Arab Emirates] that produces UAVs," and he was indicted by an Israeli court for allegedly sending e-mails with sensitive information about UASs back to HAMAS activists in Gaza.[201]

In terms of technology transfer and learning, HAMAS also likely benefited from Israeli UASs that malfunctioned, crashed or were downed in Palestinian territory from the mid-2000s onward, if not earlier. By the author's own estimate, at least one Israeli UAS has crashed in the Palestinian territories since 2009, and it is not clear if Israel's security services have been able to recover all of its downed drones. HAMAS and other groups have studied Israel's UASs so they can either reengineer or learn how to defeat them.[202]

In November 2012, during Israel's Operation Pillar of Defense, the IDF conducted strikes against "HAMAS facilities that were being used to develop drones capable of carrying explosives."[203] To legitimize its strike, the IDF posted a YouTube video that showed HAMAS activists test-flying a drone.[204]

197 Ibid. An unsourced report from *Jane's* claims that "in 2004, six members of . . . Hamas were allegedly killed when trying to make their own explosive-packed drone." See "Attack of the Drones—the Dangers of Remote-Controlled Aircraft," *Jane's Intelligence Review*, December 16, 2011.

198 For November reference, see Michael Gips's reference to the *Vremya Novostei* story in Gips, "Remote Threat." For example, according to a report by Eugene Miasnikov, in 2004 the Israeli government prevented a plot by an unnamed Palestinian extremist group "to attack a Jewish settlement in Gaza" with a UAS. As noted by Eugene Miasnikov, the original source is "*V. Izraile predotvraschvon terakt s ispol'zovaniyem BLA*," ("Terrorist Act with UAV Employment Has Been Prevented in Israel"), *Polit. Ru*, March 10, 2004. The author was not able to verify the original source or find additional reporting on this incident, however.

199 Ami Ben-David, "Temple Mount Targeted," *Ma'ariv* (in Hebrew), May 16, 2005, p. 2.

200 Meir Suissa, "HAMAS Is Trying to Build UAVs," *Ma'ariv* (in Hebrew), November 10, 2005, p. 10.

201 Ibid.

202 "Hamas Claims to Capture Israeli UAV," *Times of Israel*, August 12, 2015.

203 Gili Kohen, "HAMAS Has More Drones Up Its Sleeve, Defense Officials Say," *Haaretz*, July 14, 2014.

204 See www.youtube.com/watch?v=A3jg4fZLfxQ.

Photo Credit: Screen grab from IDF video posted to YouTube

The following year, in October 2013, a UAS plot linked to HAMAS was disrupted by Palestinian security forces in the West Bank. According to the *Times of Israel*, the cell was "in the advanced stages of planning to launch a UAV into Israel" and had already "run several test flights." The group was planning to attach explosives to the UAS so it could inflict more damage.[205]

In 2014 HAMAS launched at least two drones into Israel. The flights were conducted during the "fifty-day war" between HAMAS and Israel that summer, and they represented a number of firsts for the Palestinian group. One major step forward was that at least one of the drones, an Ababil A1B, had what HAMAS claimed were four armed air-to-ground "missiles" attached to its wings in addition to a camera. To publicize the event, the group released pictures and video taken from the UAS via Twitter, which showed the UAS, loaded with its missiles, in flight.[206]

Photo Credit: Screen grab from a HAMAS video

This prompted a debate about whether the missiles were real and could be fired or were just mock-ups added to the UAS to stoke Israeli fears.[207] As noted by one reporter, the fact that "the drone didn't use any of the onboard weaponry seems to suggest it does not have a real capability to use it."[208] An Israeli air force officer summed up the dangers posed by the HAMAS drones as follows: they "aren't super bombers, they're like model airplanes—not very large. If it takes photographs, it's 10 watts, and if it attacks, it's less than a rocket in its capabilities," he said, referring to the possibility of a suicide drone laden with explosives. The air force is prepared for such a possibility, he added.[209]

205 Issacharoff, "PA Forces Thwart Hamas Attack Drone Plot in West Bank."

206 David Cenciotti, "Hamas Flying an Iranian-Made Armed Drone over Gaza," *Aviationist*, July 14, 2014.

207 Ibid.

208 Ibid.

209 Kohen, "HAMAS Has More Drones Up Its Sleeve, Defense Officials Say."

But, as even HAMAS's spokesman acknowledged, the UAS flights were still a win, owing to their psychological impact:

> First of all, at this point in time, there is a security aspect to the launch of the drone. There is also a morale-related and symbolic aspect to the launch of this drone. With regard to the security aspect, the drone has managed to capture images of significant security and military facilities that will be used by the Al-Qassam Brigades. This is a highly significant security and intelligence achievement. The other aspect is symbolic; and it lies in the fact that the resistance has, at last, managed to launch a drone that flies over Israeli settlements in defiance of the aircraft that are flying over Gaza. It is true that these drones are still in the early stages of development. However, the fact that the Al-Qassam Brigades has [*sic*] reached this level of technological know-how indicates that these drones can be further developed to render them a match to Israeli drones in the next stage, God willing.[210]

Even if the UAS was not as capable as HAMAS touted, Israel took the issue seriously. Less than two weeks after HAMAS's July flights, the Israeli air force targeted and killed Ismael Muhammad Sa`ad Akluk, a twenty-five-year-old individual who reportedly served as "a key figure in HAMAS's drone and rocket research program."[211]

These HAMAS UAS flights also represented a first in terms of the Israeli response they elicited. While the "first drone was shot down on July 14 over the southern Israeli city of Ashdod . . .the second was intercepted three days later over the city of Ashkelon."[212] Unlike previous encounters, both HAMAS drones were reportedly downed by Patriot surface-to-air missiles, which according to the Israeli air force, "was the [Patriot] battery's first operational interception since the 1991 Gulf War."[213] Prior to that, Israel had downed HAMAS and Hezbollah UAS via other means, such as firing at them from Israeli aircraft. When one compares the low cost of HAMAS's and Hezbollah's drones to these costly Israeli countermeasures, it isn't hard to see the economic asymmetry that is at play, and how it is in these militant groups' interest—as part of a broader economic and strategic communications warfare campaign—to use these relatively cheap devices to conduct consistent flights over Israeli territory. Israel has sought to mitigate a similar problem regarding the launch of inexpensive mortars and rockets from southern Lebanon and the Palestinian territories through the deployment of its Iron Dome system (which is also an expensive system), and both Israel and the United States are currently in search of more cost-effective counter-UAS systems to deal with this exact issue. Despite this being the case, this measure-countermeasure dynamic illustrates that HAMAS's and Hezbollah's drones remain a threat not only because of the diversity they provide in terms of potential attack platforms, but also because of their small size, robust mobility and (likely) future ability to evade certain countermeasures, not to mention their ability to solicit expensive, unsustainable countermeasure responses.

Several months later, in December 2014, HAMAS flew another UAS at a rally it was holding in Gaza. Israel scrambled planes as a preventative measure, but the IAF did not strike the HAMAS UAS because the aircraft stayed in the Palestinian territories and was not viewed as a threat.[214] In February the following year, HAMAS reportedly made several UAS flights over Egyptian airspace in the Sinai Peninsula.[215] According to one source, the HAMAS UAS flew "as far as El Arish and Sheikh Zuweid, some 50 kilometers from the Egypt-Gaza border."[216] Egyptian radar reportedly "picked up the three

210 Al-Jazirah Satellite Channel Television (in Arabic), July 14, 2014.

211 Yaakov Lappin, "Hamas's Drone and Rocket Development Chief Killed in IAF Strike," *Jerusalem Post*, July 27, 2014.

212 "Israel Shoots Downs UAV over Syria Interim Border," *Philippine News Agency*, September 1, 2014.

213 Kohen, "HAMAS Has More Drones Up Its Sleeve, Defense Officials Say."

214 Yaakov Lappin, "IDF Scrambles Jets to Gaza Border After HAMAS Flies Drone," *Jerusalem Post*, December 14, 2014.

215 Stuart Winer, "Hamas Drones Said to Enter Egyptian Airspace," *Times of Israel*, March 11, 2015.

216 Ibid.

drones" but local border forces were not able to "hit them because they were flying at an altitude of 750 meters (2,250 feet)," an elevation that was too high for their small arms.[217] HAMAS is believed to have conducted the flights due to tension between it and the Egyptian government, the latter of which claimed, after the ouster of Mohamed Morsi and his Hamas-friendly Muslim Brotherhood government, that HAMAS was assisting the violent antistate actions of jihadist groups in the Sinai.[218]

The arrest and indictment of a young Palestinian Islamic Jihad activist, Majd Ouida, in February 2016 for his role in successfully hacking into the Israeli Defense Forces' UAS feeds illustrates the reoccurring and consistent challenges state actors face in trying to find the right balance between protecting their feeds and providing pathways for their operatives to also make use of that same data.[219] According to news reports, Ouida used a satellite dish and a frequency counter to hack into the IDF feeds. After identifying the UAS signal, Ouida then had to decode it; he is believed to have had access to the decoded feeds for a period of at least two years, from 2012 to 2014.[220] The feeds were beneficial to Islamic Jihad as they revealed the facilities that were being surveyed by the IDF. For the Israelis, this case almost certainly stung, as more than a decade and a half earlier Hezbollah was able to gain similar access to Israeli drones, and, as a result, to learn more about their priorities.

ISLAMIC STATE	First sign of program: 2013
UAS Use: Surveillance, external communications, weaponization	
Takeaways: Most-prolific user of commercial drones; geographic use in Iraq and Syria; creative	

Another terrorist group to show signs of a UAS program is the group that calls itself the Islamic State. While the Islamic State has not been in the UAS game as long as Hezbollah or HAMAS, and its UAS platforms are currently not as sophisticated, the frequency of the Islamic State's use of drones, and the group's employment of them across multiple locations in Iraq and Syria, warrants the inclusion of its efforts as a "program."[221]

Unlike Hezbollah and HAMAS, whose drones are usually modified versions of Iranian machines, the Islamic State has used both commercially available and homemade drones in the course of its operations. The first signs of the Islamic State's interest in drones comes from a number of news accounts that emerged in the summer of 2013, before the group severed its formal ties with al-Qa`ida, changed its name and formally declared the creation of its caliphate. In June 2013, Iraqi authorities arrested five men tied to the Islamic State who were reportedly planning to use remote-control helicopters to distribute sarin and mustard gas as part of an attack against unspecified targets in Iraq, North America and Europe.[222] They were believed to have been working in collaboration with another, unspecified

217 As noted by Stuart Winer in the *Times of Israel* article referenced in footnote 215, "Under the terms of the 1979 peace deal with Israel, Egypt is not allowed to station any anti-aircraft weapons in the Sinai region, so its forces have been unable to prevent the Hamas activities."

218 Ibid.

219 For background, see David Axe, "How Islamic Jihad Hacked Israel's Drones," *Daily Beast*, March 25, 2016.

220 For background on how he was able to accomplish this, see ibid.

221 For a general rollup of select Islamic State UAS use, see Friese et al., "Emerging Unmanned Threats," pp. 43–44.

222 For background, see David Blair, "Iraq Foils Suspected al-Qaeda Plot to Launch Remote-Controlled Helicopters Carrying Chemical Weapons," *Telegraph*, June 3, 2013; Madeleine Morgenstern, "Iraq Says It Foiled New Al-Qaeda Plot to Use Toy Planes to Drop Chemical Weapons over North America and Europe," *Blaze*, June 2, 2013; for background on Abu Musab al-Zarqawi's history of experimentation with chemical and biological agents, see Joby Warrick, *Black Flags: The Rise of ISIS* (New York: Doubleday, 2015), pp. 70, 89, 139, 144.

"offshoot" of al-Qa`ida.[223] While little details exist about the plot, and the "Iraqi government's claims have not been independently verified," the cell was reportedly uncovered as a result of "co-operation between Iraqi and foreign intelligence services."[224] Also, according to Iraqi authorities, the five men involved were monitored by intelligence units for a period of three months prior to their arrest, and as part of their operation Iraqi forces found and raided "three workshops for manufacturing chemical agents" where "toy planes were seized on site."[225] As illustrated below, the Iraqi government provided pictures of the model helicopters and lab materials to lend credibility to these claims. If substantiated, this early plot by the Islamic State in Iraq and the Levant (ISIL, a predecessor organization to the Islamic State group now led by Abu Bakr al-Baghdadi), would add credence to the concerns raised in the spring of 2016 by British prime minister David Cameron and other Western leaders that the Islamic State was planning to use drones to disperse toxic material over cities in the West.[226]

Photo Credits: Screen grabs from BBC

Then, in March 2014, several months before the formal creation of the so-called Islamic State in June 2014, the al-Minbar al-I'lami jihadist forum released a short video titled "Drone Belonging to the Al-Fallujah Mujahidin Today," which showed a UAS in flight.[227] The video claimed that the UAS shown in it had been manufactured by ISIL.[228]

The Islamic State's first big UAS reveal, however, occurred five months later. As in August 2014, the group posted a video to YouTube that showed aerial footage of a Syrian air base taken from a commercial drone (a DJI Phantom).[229] The release of the video followed, and was designed to celebrate, the Islamic State's takeover that same month of the base it had surveyed from the air. As noted by Colin Clarke, the Islamic State used the UAS "as a recon method to scout out what the base looked like before going in with a more kinetic attack."[230] After identifying sensitive or vulnerable areas, they then "used multiple suicide bombers to gain entry" to take over the facility.[231] The group's takeover of the facility was noteworthy because it was located in Raqqah, the area which now serves as the group's headquarters and main stronghold. The Syrian base also reportedly contained a number of surface-to-air missiles.[232]

223 Morgenstern, "Iraq Says It Foiled New Al-Qaeda Plot to Use Toy Planes to Drop Chemical Weapons."

224 Blair, "Iraq Foils Suspected al-Qaeda Plot to Launch Remote-Controlled Helicopters Carrying Chemical Weapons;" Morgenstern, "Iraq Says It Foiled New Al-Qaeda Plot to Use Toy Planes to Drop Chemical Weapons."

225 Morgenstern, "Iraq Says It Foiled New Al-Qaeda Plot to Use Toy Planes to Drop Chemical Weapons."

226 For background, see Ben Riley-Smith, "ISIL Plotting to Use Drones for Nuclear Attack on West," *Telegraph*, April 1, 2016.

227 User "Al-Murabit," "First Surveillance Drone Manufactured by ISIL," Al-Minbar al-I'lami Jihadist Forum (in Arabic), March 21, 2014.

228 Ibid.

229 For background, see Peter Bergen and Emily Schneider, "Now ISIS Has Drones?" CNN, August 25, 2014.

230 Yasmin Tadjdeh, "Islamic State Militants in Syria Now Have Drone Capabilities," *National Defense*, August 28, 2014.

231 Ibid.

232 Thomas Gibbons-Neff, "Islamic State Might Have Taken Advanced MANPADS from Syrian Airfield," *Washington Post*, August 25, 2014.

Photo Credits: Screen grabs from Islamic State videos

Two additional events took place toward the end of 2014 that further revealed the reach of the Islamic State's drones. In November of that year, the Syrian army reportedly shot down an Islamic State UAS that was conducting surveillance in eastern Syria, in Deir Ezzur province.[233] Then in December, the group posted another video online that showed aerial footage of Kobane, a town that sits along Syria's northern border with Turkey and that the group controlled for a period. In its video of Kobane, the Islamic State used the UAS to show "wide sweeping shot[s] of the town… [and to] tag the locations of three of its suicide attacks against Kurdish and rebel Free Syrian Army ground troops" in a visually slick way.[234]

Photo Credit: Islamic State video

In 2015 there was more of the same, including three incidents that happened over the course of several months in the spring. For example, in March 2015 the United States conducted an airstrike against a vehicle near the Sunni jihadist hotbed of Fallujah, Iraq, after it was linked to an Islamic State UAS flight. According to a U.S. military spokesperson, the vehicle was targeted because the fighters who entered the vehicle had been flying a drone, which they were using to conduct "surveillance along IS front lines."[235] (Since that strike the U.S. military has conducted at least eight additional airstrikes to destroy other Islamic State drones.[236])

The following month, copying the technique the group used to aid its takeover of the Syrian air base in Raqqah, the Islamic State used a UAS to conduct surveillance of a major oil refinery in Baiji, Iraq.

233 "Syria: Army Downs ISIL Drone in Deir Ezzur," Fars News Agency, November 30, 2014.

234 Ruth Sherlock, "Islamic State Release Drone Video of Kobane," *Telegraph*, December 12, 2014.

235 "US Says It Struck Islamic State Drone in Iraq," Associated Press, March 18, 2015.

236 Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones," *New York Times*, October 11, 2016.

During this episode, the group used the UAS "to gather intelligence… for command and control purposes, as well as act as spotters [*sic*] for artillery pieces" they used.[237] A video the Islamic State released also showed several of its fighters sitting in an "operations control room," which the group claimed was being used to coordinate its assault against the oil facility.[238] Then in May 2015, Kurdish Peshmerga forces reportedly shot down an Islamic State UAS that was surveilling Kurdish forces outside Erbil.[239] The Iraqi police shot down another UAS outside Ramadi in October 2015.[240]

According to an unconfirmed Facebook post created by a user on the page of the Kurdish "People's Defense Units" (also known by its Kurdish acronym, YPG), in mid-December 2015 Kurdish units shot down an Islamic State UAS, and watched another one loaded with explosives detonate.[241] The user posted a number of pictures of the UAS that the Kurdish unit had allegedly shot down.[242]

Photo Credit: Friends of the YPG/YPJ

Metadata from those pictures suggest that the Kurdish unit recovered the UAS near the Syrian town of Kobane.[243] While the exact version of the UAS has not been confirmed, "some eagled-eyed redditors believe the drone in question… is the Skwalker X7 or X8, which costs $179 for the kit."[244] If confirmed, this case would be the first time the Islamic State successfully weaponized a UAS.

The Islamic State made additional advances in 2016. In March of that year the Islamic State flew a commercial drone over a "newly created series of bases in Northern Iraq where American and Iraqi forces were stationed."[245] Not long thereafter the Islamic State fired a Katyusha rocket into the middle of one of those bases, where more than 100 American Marines were stationed, and the blast killed one of them.[246] The accuracy of the strike, which some "military officials described… as a "golden shot"

237 Caleb Weiss, "Islamic State Uses Drones to Coordinate Fighting in Baiji," Long War Journal, April 17, 2015. As noted by Weiss, it "is unclear what kind of unmanned aerial vehicles were employed by the group."

238 Ibid.

239 "Peshmerga Shoot Down Islamic State Drone in Gwer," *Iraq News Today*, May 5, 2015.

240 "Iraqi Police Shoots Down ISIS Drone East of Ramadi," Defense Blog, October 3, 2015.

241 David Hambling, "ISIS Is Reportedly Packing Drones with Explosives Now," *Popular Mechanics*, December 16, 2015.

242 Ibid.

243 Ibid.

244 Ibid.

245 Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones."

246 Ibid.

to pierce the defenses put in place," led some to speculate "that the drone was used in the targeting."[247] Other U.S. military officials suggested that the timing of Islamic State surveillance flight and the strike was only a coincidence.[248]

In 2016, the Islamic State also deployed several commercial drones that they had weaponized, and they did so on at least three occasions during a one month period between September and October of that year.[249] In each of these three cases the Islamic State attached explosives to a drone and sought to use the platform as a mechanism to deliver an improsived explosive device.[250] While the first two incidents were of limited impact, the Islamic State's third attempt resulted in the death of two Kurdish fighters.[251] It also seriously injured two French Special Force soldiers.[252] To inflict these casualities, the Islamic State used deception, as it is believed that the "explosive device inside [the UAS] was disguised as a battery."[253] And so after Kurdish forces shot down the drone, the two fighters who were inspecting it received a nasty, and lethal surprise.[254] It is not known if the deceased Kurdish fighters set off the explosive accidently or if the device was detonated remotely by Islamic State fighters operating nearby. This incident is noteworthy as it is the first confirmed case of a weaponized drone operated by a terrorist group contributing to actual deaths.

Despite the group's ability to deceive and leverage its UAS exploits through slick and well-publicized media releases, the drones flown by the Islamic State are not that advanced. Indeed, as noted by David Cenciotti, "when it comes to drones, Islamic State is no more sophisticated than your average hobbyist."[255] The success of the Islamic State's UAS efforts have been bolstered, and tied to, the more permissive UAS environment in which the group has operated, as the group's two seminal UAS flights over the Syrian air base in Raqqa and the contested city of Kobane attest. Further, the UAS variants used by the group, which are mostly commercial or homemade, are easy to jam or take control of remotely, assuming forces on the ground see or hear them coming. Thus, at this point the danger of the Islamic State's UAS use lies less in the type and sophistication of the platforms it possesses and more in the sheer number of them and the group's ingenuity—and specifically how, where and in what novel way the group will use drones in the future. The group's media-savviness and the 2013 Iraqi press reports about the interests of the Islamic State's predecessor group in chemical-biological UAS applications are particularly concerning in this regard, as is the group's more-extended history of experimentation with these types of weapons.

247 Ibid.

248 Ibid.

249 Ibid.

250 Ibid.

251 Ibid.

252 "Islamic State Drone Kills Two Kurdish Fighters, Wounds Two French Soldiers," Reuters, October 12, 2016.

253 Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones."

254 Ibid.

255 David Cenciotti, "Islamic State has Drones: Nobody Panic," *Medium*, September 2, 2014.

JABHAT FATEH AL-SHAM	First sign of program: 2014
UAS Use: Surveillance, external communications, weaponization* (*through alliance w/ Jund al-Aqsa)	
Takeaways: UAS program not as active as Islamic State; geographic use in Syria	

The last group that has demonstrated repeated use of drones is the Sunni jihadist group Jabhat Fateh al-Sham. As documented by Larry Friese et al., Jabhat Fateh al-Sham's first known use of a UAS occurred in October 2014, when the group "released a propaganda video highlighting" footage taken from a commercially available UAS that it used in its efforts "in breaking the siege of al-Maliha."[256] The character and style of the UAS footage that Jabhat Fateh al-Sham incorporated were quite similar to the video that the Islamic State released several months earlier, which suggests that Jabhat Fateh al-Sham might have been inspired by that group's stylish drone video and sought to mirror the Islamic State's technique. Jabhat Fateh al-Sham has also used commercial drones on at least two other occasions: to highlight the group's battles around Aleppo and to document a suicide attack "and a subsequent assault on Shi`a enclave towns in Idlib governorate under siege by Nusra and other anti-regime forces."[257]

Jabhat Fateh al-Sham screen grab of UAS footage over al-Maliha, Syria (Larry Friese et al.[258])

Jabhat Fateh al-Sham's drone operations will also benefit from the achievements of Jund al-Aqsa, a Syrian-based militant group with whom it formally merged in October 2016, as in September of that same year Jund al-Aqsa dropped explosives from a commercial UAS.[259] This means that Jabhat Fateh al-Sham now has this capability too.

Assessment

The cases reviewed shed light onto four dimensions of the UAS terror threat: (1) where drones have been used; (2) the type of groups that have experimented with them; (3) the timing of UAS programs;

256 Friese et al., "Emerging Unmanned Threats," p. 45.

257 Ibid.

258 Ibid.

259 Thomas Joscelyn, "Jund al Aqsa Used Drone to Drop Small Bomb on Syrian Regime Force," ThreatMatrix blog, September 2, 2016; "Jund al-Aqsa Pledges Allegiance to ex-Qaeda Branch in Syria," *Al-Arabiya* (English), October 9, 2016.

and (4) how and to what effect UAS platforms have been employed by terror entities.

Geographic Proliferation of UAS Use

As figure 3 illustrates, the four terror groups that have identifiable UAS programs—Hezbollah, HAMAS, the Islamic State and Jabhat Fateh al-Sham—are geographically concentrated. All of these organizations are based in the Levant and are primarily active in the Middle East. It is also worth pointing out that two of these groups, Hezbollah and HAMAS, have historically been supported by Iran, indicating that Iran has been a key enabler of nonstate terror use of UAS technology.[260]

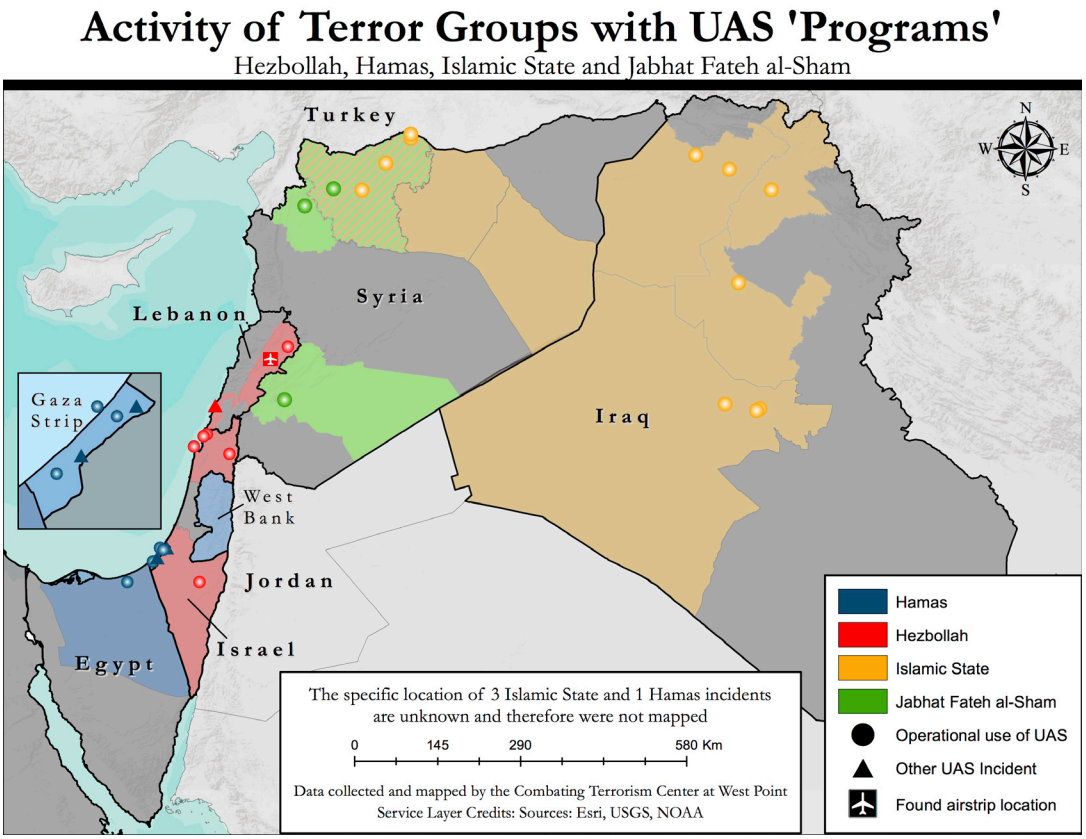

Figure 3: Geographic Overview of Terror Group UAS Program Activity

When one looks beyond groups with UAS programs, and focuses instead on the proliferation of drone possession or use by all terror-linked entities, the picture that emerges is more geographically diverse. As figure 4 demonstrates, terror entities' interest in using drones to support their operations spans the globe and includes incidents that have occurred in Colombia, Egypt, Germany, Iran, Iraq, Israel, Japan, Lebanon, Pakistan, Palestine, Spain, Syria and the United States.

260 The other group that could potentially have a UAS program is Laskhar-e-Taiba, an entity that has historically been supported by a state (Pakistan), but the author could not find enough evidence of repeated UAS use to warrant LeT's inclusion in the program category.

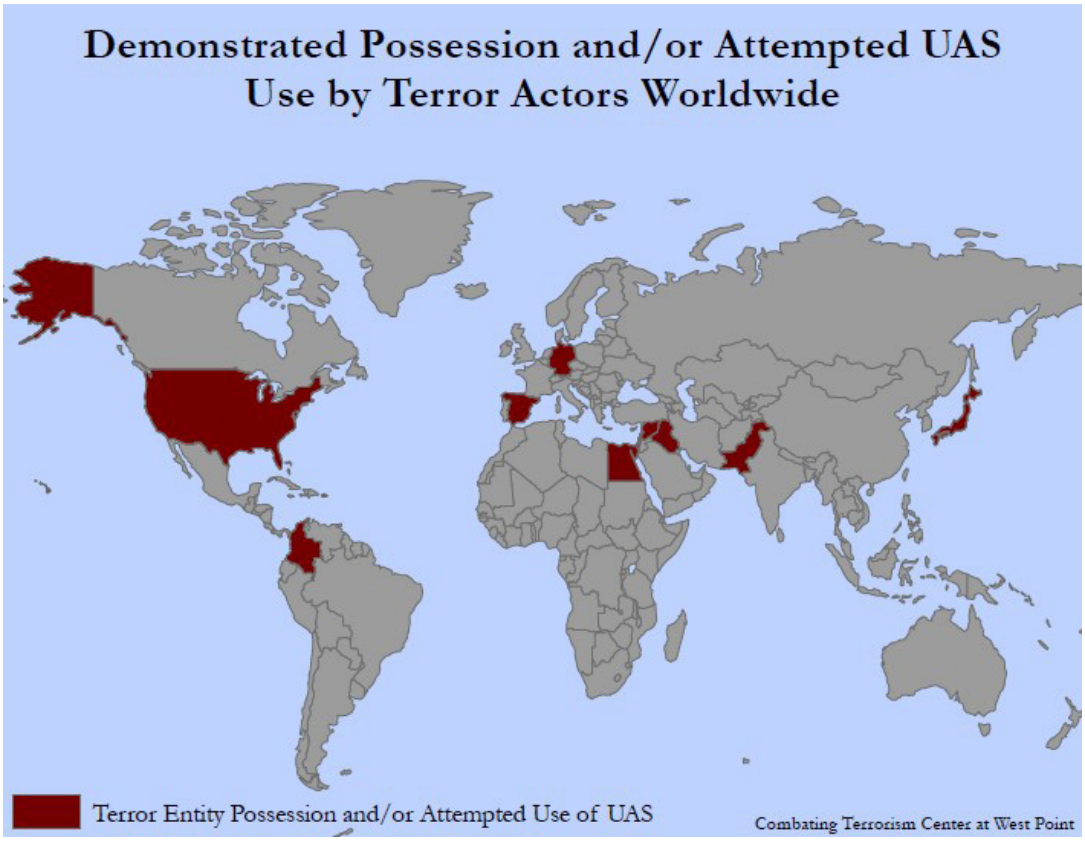

Figure 4: Global Proliferation of Demonstrated UAS Terror Possession or Use

Group Types and Organizational Dynamics

The type of terror organizations that have demonstrated an interest in drones is also ideologically diverse. While the cases reviewed above are heavily skewed toward those inspired by radical conceptions of Islamic ideology (from both Sunni and Shi`a schools of thought), terrorist use and interest in UASs also spans entities motivated by apocalyptic, right-wing and irredentist ideologies. This suggests that future terror group use of UAS technology will not be limited to just one type of extremist ideology, but will likely involve many.

The four groups with identifiable UAS programs all hold physical terrain and operate from areas that they control. This suggests that a terror group's ability to develop a weapons development program, including a UAS program, could be tied to its ability to seize and hold terrain, and to maintain control over a stable territorial base—even if small.[261] Members of all four groups have also been the target of drone strikes, a factor which could have incentivized each group to develop tools that would allow them to strike back at their enemies using similar technology.

Another characteristic that is common among the four groups with UAS programs is their age. Three of these entities have organizational histories that stretch back more than a decade, meaning that they are seasoned and not young. Even though Jabhat Fateh al-Sham is technically not as old, it has benefited from the advice provided by a number of seasoned operatives who had decades-long expe-

261 I thank my colleague Arie Perliger for this point. Credit is to him.

rience with other organizations (i.e., al-Qa`ida core).[262] Other groups that showed an early interest in drones, such as Aum Shinrikyo, FARC, LeT and the Haqqani Network, are also those that are more mature and have a track record of innovative behavior.[263]

Group	Hezbollah	HAMAS	Islamic State*	Jabhat Fateh al-Sham
Founded	1985	1987	2004	2011
Age	31	29	12	5

** 2004 is the founding of the IS's predecessor organization, al-Qa`ida in Iraq*

One noteworthy exception to this collection of older groups that are UAS users is the Liberation Tigers of Tamil Eelam (LTTE). The lack of data indicating LTTE experimentation with drones came as a surprise, especially since the group is well known for its innovative practices, including its use of maritime suicide operations.[264] One potential explanation for LTTE's absence in this area is that instead of investing in unmanned aerial systems, it decided to prioritize and devote resources to the development of manned platforms, a decision that, as the group's successful bombing of a Sri Lankan air base with planes that it smuggled into and then reassembled in its territory demonstrates, proved operationally effective.[265] Another potential explanation is time, as the period when commercial drones were becoming both more capable and available aligns with the period when LTTE was beginning to struggle as an organization.[266]

Another surprise was that only one of the thirteen individual cases reviewed for this report (the case of Christopher Paul) had a proven tie to al-Qa`ida. Another small three-person group in Gibraltar was rumored to have the same, and yet another individual (Rezwan Ferdaus) believed that he was operating on behalf of al-Qa`ida, even though he was communicating only with representatives of the FBI. While the Turkistan Islamic Party is allied with and often operates in association with al-Qa`ida affiliated elements in Syria, that group has its own identity. Further, besides the four cases directly associated with the Islamic State, the author was unable to find evidence of any Islamic State–inspired, individual UAS plots outside the caliphate. Given the trajectory of the Islamic State, and that group's call for inspired sympathizers to act independently in their home countries on behalf of the group, this could change.[267]

Timing Considerations and UAS Terror Threat Evolution

Terrorist interest in drones is anything but new. While terror groups' interest in and use of drones has become more frequent over the last ten years, especially as commercial systems and associated technology have become more popular, sophisticated and accessible, the first terror UAS case occurred

262 For background, see Jennifer Cafarella, "Jabhat al-Nusra in Syria: An Islamic Emirate for al-Qaeda," Institute of the Study of War, *Middle East Security Report 25*, 2014.

263 For background, see Adam Dolnik, "Aum Shinrikyo," in *Understanding Terrorist Innovation: Technology, Tactics and Global Trends* (New York: Routledge, 2007), pp. 58–80; Bruce Reidel, "Mumbai Terror Attack Group Lashkar e Tayyiba Now More Dangerous Than Al Qaeda," *Daily Beast*, July 1, 2012; "Haqqani Network's Reign of Terror on Afghanistan," NPR, September 3, 2009.

264 "100 Rebels Slain in Battle with Sri Lankan Navy," *Washington Post*, October 20, 1997; Amy Waldman, "Masters of Suicide Bombing: Tamil Guerillas of Sri Lanka," *New York Times*, January 14, 2003.

265 "LTTE Planes Bomb Military," *Dawn*, October 29, 2008; Jyoti Thottam, "A Surprise Attack by Sri Lanka's Tamil Tigers," *Time*, February 20, 2009.

266 For background on LTTE's decline, see Peter Layton, "How Sri Lanka Won the War," *Diplomat*, April 9, 2015.

267 Mitchell Prothero, "Islamic State Spokesman Calls for 'Lone-Wolf' Attack in the West," McClatchy, June 30, 2014; the Islamic State has also reportedly called on its followers to outfit commercial drones with explosives, see Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones."

more than two decades ago. Figures 5 and 6 visualize the trajectory of UAS terror capabilities, as represented in relation to UAS programs and individual cases, and show how this phenomenon has evolved since Aum Shinrikyo first experimented with the technology. While the solid lines in each graphic demonstrate the first UAS incident for each organization or case, the categories on the left axis are a capability scale that ranges from interest in drones at the bottom to the successful weaponization of a UAS at the top. Additional incidents related to a specific group are case are annotated by dotted lines.

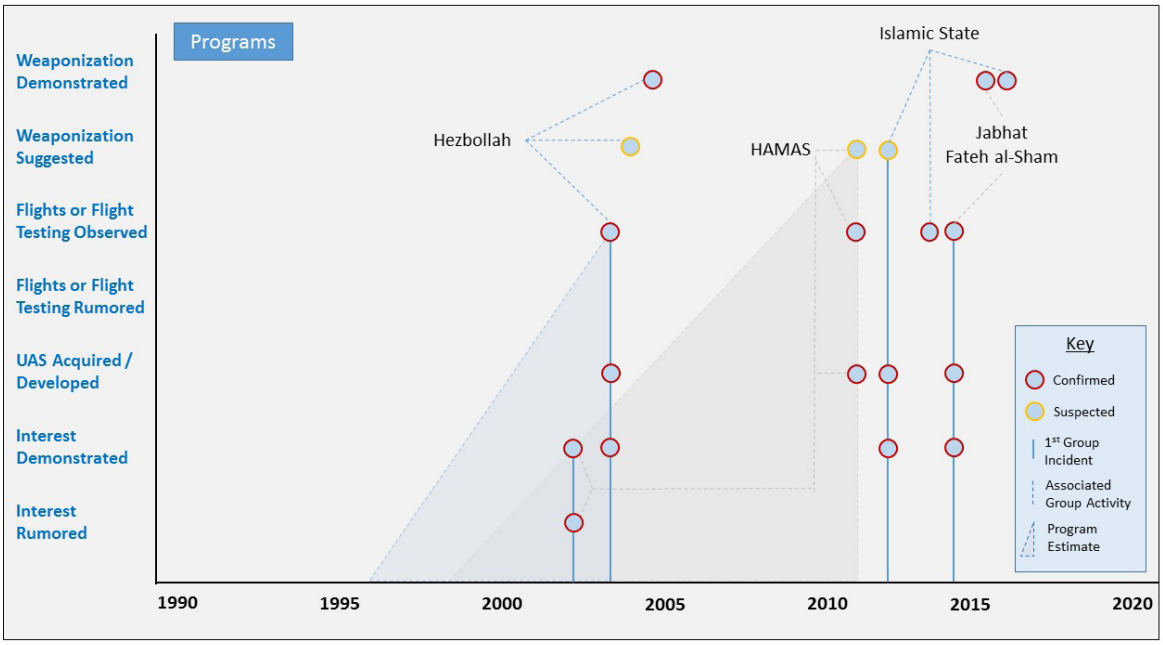

Figure 5: Timeline of UAS Terror Group Programs

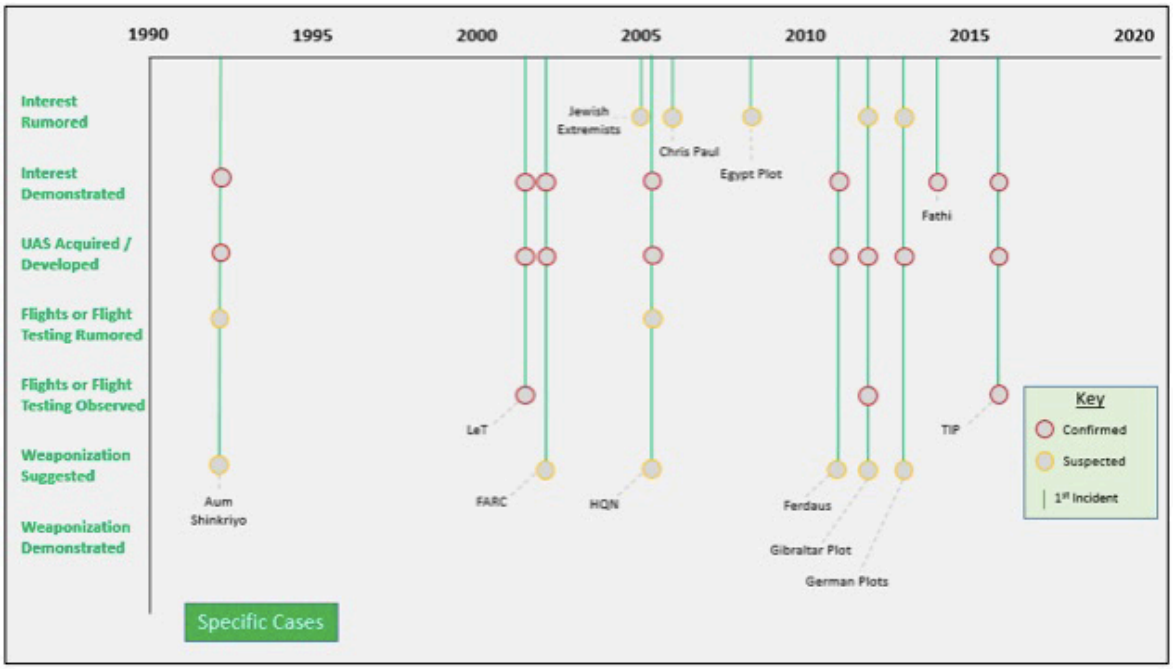

Figure 6: Timeline of Individual UAS Terror Cases

The lack of information on the internal decisionmaking of terrorist groups, the limited number of cases of terrorist use of drones and the diversity of UAS capabilities across groups makes it difficult to make concrete judgments from these graphics; among these difficulties is judging the time it takes an organization to develop a UAS program. Indeed, a comparison of Hezbollah's and the Islamic State's UAS programs reveals that not all terror UAS programs are created equal. For example, even though the available evidence indicates that the Islamic State has been able to "ramp up" its program in considerably less time than Hezbollah took to develop its program (likely in part due to the more common availability of commercial UAS platforms over the last decade), the UAS capabilities of the latter group are much more robust. Based on what is known, Hezbollah seems to have taken seven years from its initial, demonstrated point of UAS interest (the Ansariya ambush in 1997) to the successful deployment of a UAS in flight during an operation (i.e., a cross-border flight into Israel in 2004 that required enhanced range and control capabilities).

While data about the Islamic State's early interest in UAS are less clear, the time between the first public indications of that group's interest in the technology (2013) to its first known operational deployment of a UAS (2014) was much shorter. Yet despite these potential differences, the data also speak to similarities between these two programs. For example, both groups took approximately two years from their first, public operational use of a UAS for reports to emerge that they had loaded a drone with explosives.

The maturation of data concerning terror UAS use over time, and an increase in terrorism-related cases, will provide additional insight into these questions, and refine our understanding of how terror UAS programs evolve.

Overview of Terror UAS Capabilities—Strategic Communications, Weaponization and Flights

A fourth area of the cases reviewed concerns how, and to what effect, terrorists have used drones. The data reveal that while many groups or individuals have shown an interest in the technology, few have successfully deployed it in any meaningful way. Terrorists' use of drones has certainly complicated some conflicts, but the use of this technology by terrorists has yet to change or significantly alter the direction of any conflict, and so the broader impact of this tool thus far has been quite limited.

Drones have been primarily used by terror entities for surveillance and strategic communications purposes, and it is in this area where terrorists have made the most gains. One factor that was observed in a number of cases was the quick tendency of the media to hype terror UAS incidents even when no demonstrated threat existed, an issue that could push terror groups to select drones over other options in the future.[268]

Besides Hezbollah, the Islamic State, and Jabhat Fateh al-Sham no other terror groups or terror-linked individual are believed to have successfully used a weaponized UAS to date in an operation.[269] The Islamic State, at the time of writing, appears to be the only group that has used a weaponized drone to kill. HAMAS has also reportedly flown a weaponized drone, but it has yet to succeed in using a UAS in a lethal way as part of an attack. There have also been seven other times when a group or individual both possessed a UAS and the weaponization of that device appears to have been a goal. These plans or plots did not transpire for two main reasons: the perpetrator selected a different delivery mechanism (one case) or the use of the device was thwarted by state authorities (six cases). Further, besides the four groups with UAS programs, only three other entities—Lashkar-e-Taiba, the Turkistan Islamic Party, and the three-person Gibraltar clique with alleged ties to al-Qa`ida—appear to have successfully

268 I thank Arie Perliger for pointing this issue out to me.

269 Given its October 2016 merger with Jabhat Fateh al-Sham, the September 2016 incident during which Jund al-Aqsa used a UAS to drop a small bomb on Syrian regime targets has been included as a Jabhat Fateh al-Sham event. For background, see Joscelyn, "Jund al Aqsa Used Drone to Drop Small Bomb on Syrian Regime Force."

conducted UAS test flights.

Limiting Factors: Technical Features, Specific Choices and Countermeasures

Three reasons explain the inability of terrorist entities to inflict a significant amount of casualties using a drone to date. First are the limitations associated with the range, endurance and payload of commercially available drones, which are the devices believed to have been used in the cases reviewed above, with Hezbollah, and potentially HAMAS, being the exceptions. Range and endurance limitations put this into perspective. For example, an analysis of "202 commercially-available drones listed on the product comparison site SpecOut.com" conducted by the Remote-Control Project "reveals that the listed drones have an average flight time of 18 minutes, an average range of 1,400 meters and median price of $600."[270] As noted by the Remote-Control Project team: "This means a pilot must be within a particular proximity of the UAV and that flights cannot span a significant distance."[271]

Second are the specific choices made by terrorists. This can be understood across a number of different levels. Take for example, the issue of commercial UAS payloads. The load-carrying capacity of commercial drones varies and ranges from less than a kilogram to several kilograms. So while the majority of commercially available systems do not have much lift capacity, models exist that could be modified to carry several kilograms of a high-yield explosive, which is enough material to cause a significant amount of damage. (For an overview of the range and payload-carrying capacity of a number of commercial drones, see the appendix).[272] This means that groups like the Islamic State either are not selecting the "right" commercial UASs—which could be a purchase, supply or acquisition problem—or they have failed in their attempts to outfit a UAS with the proper amount of explosives, or in the detonation of the device itself, which is a capability problem. The fact that Hezbollah has been able only to drop two small bomb-type munitions from a UAS, and allegedly fire rockets from another (an incident that has not been independently verified), suggests that for Hezbollah and other groups, matching capability with equipment has been a central problem.

Another dimension lies in other operational decisions made by those intent on committing terror. As Rezwan Ferdaus's failed UAS attack plot illustrates, sometimes terrorists make bad choices. In Ferdaus's case, that meant being duped into believing that he was actually interacting with representatives of al-Qa`ida when instead he was talking to an agent of the FBI. The last way in which terrorist choice has contributed to the lack of successful armed terror UAS attacks lies with groups selecting other, more conventional and less complicated attack options (i.e., the gun or the bomb) over one that uses a drone. The rationale in selecting the former over the latter is clear: more-traditional attack options are easier and ensure a greater chance of success. This seems to be particularly relevant, especially when one considers that the majority of attempts to weaponize a UAS have been tied to cases of either groups or individuals inspired by radical conceptions of Islam that embrace martyrdom. In practical terms, having members willing to volunteer for suicide operations has meant that such groups have other effective options, and these groups may not have as strong as a need to invest as heavily in armed UAS capabilities, because they can achieve casualties in other, more reliable ways.

A third major limiting factor are the countermeasures and systems that states have developed to defeat hostile drones and small, low-flying cruise missiles. Indeed, just as terrorists' interest in drones has an extended history, so too does states' interest in technology to counter such a threat. For example, the U.S. government has been concerned about this threat, and has sought ways to manage it, since

270 Abbott et al., "Hostile Drones," p. 4.

271 Ibid., p. 5.

272 See also Julio Ventura, "5 Drones that Can Lift Heavy Weights," June 16, 2016, DronesGlobe.com; "How Much Weight Can Delivery Drones Carry," Unmanned Cargo, September 29, 2015.

at least 2002.[273] Israel has also had to deal with the threat posed by small drones for over a decade, and it has deployed systems, like its "Drone Guard" technology, to identify drones and render them incapable of completing their mission.[274] Other nations, like France and Britain, are also investing in similar systems.[275] The emphasis and importance that is being given to this issue can also be seen through the counter-UAS competitions that the U.S. military has sponsored through major defense contractors and the Naval Postgraduate School, as well as in the cyber tools that the U.S. Army has created to disable rogue UASs.[276] The lack of strong encryption found in many commercial drones, as well as other vulnerabilities, has contributed to the development of a number of capable counter-UAS systems. The result is a measure-countermeasure technology dynamic that places terrorists in direct competition with their adversaries. Similar to the technology race that occurred in Afghanistan and Iraq over the use of improvised explosive devices by insurgents, this competition will see innovation from both sides, and it will take place over years.

The aggregate effect of these three limiting factors—the limitations of commercial drones, the choices made by terrorists and state countermeasures—explains why no terrorist entity to date has demonstrated UAS capability that would be considered highly capable, highly lethal and highly secure.[277]

This does not mean that there is no room for surprises, that these challenges and obstacles are insurmountable or that with a little ingenuity they cannot be overcome. One great example is Maynard Hill's successful flight of a commercially modified UAS across the Atlantic Ocean, a feat that he and his team achieved in 2003 with an 11-pound UAS, an autopilot system and less than a gallon of gas.[278] Hill and his team *were* experienced UAS hobbyists, but their feat illustrates that there are ways to leverage commercial technology to significantly extend a UAS's range. (Five years prior, in August 1998, the Aerosonde robotic airplane, a UAS that was developed by the drone manufacturer Insitu in partnership with another entity, made the same crossing. The "trans-Atlantic crossing project," which sponsored the effort, was supported by a number of defense contractors and the U.S. Office of Naval Research.[279])

Automation, which is a feature that is increasingly being incorporated into commercial drones, also provides opportunities for terrorist entities to achieve select tasks, to remove the human pilot and to limit or remove a system's dependence on external infrastructure.[280] The integration of various types of autonomous technology into commercially available UASs, like DJI's Phantom 4 drone, makes it easier for the user to track individuals (e.g., a runner that the UAS operator wants to film) and to avoid and navigate around obstacles (so the drone doesn't crash as easily).[281] As researchers at the University of Zurich demonstrated in 2015, UASs can also be programmed to autonomously navigate from

273 Bradley Graham, "Cruise Missile Threat Grows, Rumsfeld Says," *Washington Post*, August 18, 2002. Service publications and exercises also reveal that people within these communities are aware of and are thinking about these threats. See Col. Shannon W. Caudill and Maj. Benjamin R. Jacobsen, "Nowhere to Hide: The Growing Threat to Airbases," *Air and Space Power Journal*, May–June 2013.

274 For background, see "IAI Unveils 'Drone Guard': Drone Detection and Disruption Counter UAV Systems," Israel Defense website, February 18, 2016.

275 Beth Stevenson, "Anglo-French Consortium to Develop Anti-UAV System," Flight Global website, June 26, 2015; see also Brooks Tigner, "France Seeks New Counter-UAV Capability," *Jane's Defence Weekly*, January 21, 2016.

276 For example, see "The MITRE Challenge: Countering Unauthorized Unmanned Aircraft Systems," www.mitre.org/research/mitre-challenge; "Dogfighting Drones—Swarms of Unmanned Battle-Bots Take to the Skies," airforce-technology.com, July 23, 2012; and Jason Reagan, "SecDef Zaps a Drone with Army Cyber Rifle," DroneLife.com, March 30, 2016.

277 For an analysis of blast radius limitations given payload restrictions of commercial UAS, see Jackson et al., *Evaluating Novel Threats to the Homeland*," p. 21.

278 Emily Sohn, "Model Airplane Flies the Atlantic," Student Science, December 15, 2003.

279 For background, see Rob Harill, "Aerosonde Robotic Plane Completes Historic Trans-Atlantic Flight," UW Today, August 21, 1998. See also "UAV Breaks Record with Transatlantic Crossing," Flight Global, September 2, 1998.

280 I would like to thank Paul Scharre for his feedback and guidance on this issue.

281 Ben Popper, "DJI's Revolutionary Phantom 4 Drone Can Dodge Obstacles," Verge, March 1, 2016.

point A to point B without having to rely on external data linkages like GPS.[282] Removing a drone's reliance on GPS would complicate a state's ability "to jam or spoof a drone's guidance signal, because it wouldn't be relying on one."[283] There are still a number of other ways that state actors can control or bring down drones, however.[284] And the outfitting of commercial drones with autonomous features is also a two-way security street, as just as autonomous controls could create new opportunities for terrorists, other security features that are being embedded in drones, such as preprogrammed no-fly zones, which in theory preclude a UAS from being able to operate over a sensitive area, are going to make the use of them in certain areas more difficult.[285]

Existing payload limitations can also be overcome. Indeed, one of the creative options the U.S. military considered to get more reconnaissance and armed drones into the sky after 9/11 was to modify small fixed-wing aircraft, such as Cessna models, with autopilot and extended range-control systems, which would have turned those planes into drones.[286] (The trade-off for a terrorist group is that such an approach requires a runway [i.e., more-identifiable infrastructure], which would make them more prone to targeting.) Localized air defense and offensive cyber tools are also only as good as where they are placed and (if not automated) how they are manned, indicating that even with the future and potentially broad use of these UAS-defeating tools, vulnerabilities and seams will remain. All of this is to say that just as terror capabilities are limited, so too are the systems designed to defeat them.

Threat Summary

As a result of these issues, some have argued that the current threat associated with terrorists' use of drones as an attack platform is a "niche" threat and remains low, especially when compared with the relative novelty of drones to attacks that incorporate more conventional and popular weapons such as small arms and improvised explosive devices.[287] This is a hard case to argue against, as while this report has uncovered a considerable amount of evidence to illustrate that terrorist actors have long been interested in drones as an attack platform, and that those with the aspiration to use the technology are not "niche," the successful employment of drones for terrorist use has been the exception and is not widespread. Most drones have been used by terrorist organizations for surveillance or for strategic communications purposes, to publicize their ability to penetrate a denied area, to collect intelligence or to instill fear in their enemies. Further, as noted by analysts at RAND, "as long as options such as suicide operatives or vehicle bombs can be used, these more-basic and more-reliable means will generally make it possible to deliver more potent payloads to desirable targets."[288] Yet "the fact that UAVs… enable *aerial* attack does make them stand out, particularly for adversaries that might not otherwise have the ability to attack from the air. The ease of launch and potentially long-duration flight for some of these systems can be a major capability improvement for some adversaries, particularly non-state groups."[289]

---

282 See "The Smart Drones That Can Fly Themselves without GPS," ZDNet, March 20, 2015.

283 Personal communication with Paul Scharre, August 2016; for background on the concepts of jamming and spoofing of drones, see Chris Bing, "Why Hobbyists' Drones Are So Easy to Hack," FedScoop, June 16, 2016.

284 For examples, see Jordan Golson, "Army's New Laser Cannon Blasts Drones Right out of the Sky, Even in Fog," *Wired*, September 5, 2014; Lisa Vaas, "Sound: Yet Another Way to Smack Down Drones," Naked Security, August 6, 2015; Thomas Fox-Brewster, "Watch GPS Attacks That Can Kills Drones or Bypass White House Ban," *Forbes*, August 8, 2015; Mindy Weisberger, "Drone-Hunting Eagles Can Snatch Devices Out of the Sky," CBS News, February 8, 2016.

285 Fox-Brewster, "Watch GPS Attacks That Can Kills Drones or Bypass White House Ban."

286 Dave Moniz, "Old Planes Eyed as Drones," *USA Today*, February 4, 2002.

287 Jackson et al., *Evaluating Novel Threats to the Homeland*, p. xvi.

288 Ibid., p. 27; see also Lynn E. Davis, Michael J. McNerney and Daniel Byman, "Armed Drone Myth 1: They Will Transform How War Is Waged Globally," RAND Blog, February 17, 2015.

289 Jackson et al., *Evaluating Novel Threats to the Homeland*, p. 27; for another perspective, see also Davis, McNerney and Byman, "Armed Drone Myth 1."

When viewed in general terms, the current threat of a terrorist entity using a single UAS navigated via remote control should therefore be considered a moderate probability, and one with low-to-moderate consequences in terms of lethality.[290] And while any future terror UAS attack will certainly be novel and noteworthy, and help a group gain additional publicity, such an attack is unlikely to be strategic in nature—unless a UAS is used by a terror entity to successfully carry out a targeted assassination of a well-protected, high-profile figure; to kill individuals in or gain significant access to a heavily denied area, such as the White House or Israel's Negev Nuclear Research Center; to successfully disperse chemical, biological or radiological weapons; or to use the UAS in such a shock-inducing, well-publicized or creative way, perhaps combined with other weapons systems in an urban environment or at large event, that the ingenuity of the attack itself would lend itself to being strategic.

The number and sophistication of the drones used is also likely to enhance the scope and seriousness of the threat, and affect the consequence of future incidents. For example, a UAS attack that involved the use of a small group of drones, or a swarm that worked cooperatively and was guided by autonomous features, has the potential to up the ante in terms of an attack's lethality, its psychological impact and its complexity.[291]

One only needs to look at LeT's multipronged attack in 2008 on the megacity of Mumbai and the follow-on attack that David Headley and Ilyas Kashmiri were plotting in Denmark against the office of *Jyallands-Posten* to see how a UAS, or a group of them, could be creatively integrated into a more complex plan. For example, during the Mumbai attack, LeT used Secure Voice over Internet Protocol (SVOIP) systems to enable direct communication between the attackers and their Pakistan-based handlers, which provided the gunmen with added situational awareness and a direct line of support. The strategic nature and impact of LeT's 2008 Mumbai attack lay not with the use of one system in particular, but in how the group combined multiple systems and approaches (i.e., tactics, weapons, technology and hitting distributed attack sites) to enhance the operation's effect. The failed *Jyallands-Posten* plot provides an equally chilling window into how terror organizations could use a UAS to augment a violent incident. A key element of that plot was for the attackers to behead *Jyallands-Posten* employees and to throw their severed heads out of office windows so they could be put on public display in the square below. While drones were not a component of that plot, it isn't a stretch to imagine how a live video shot by an accomplice nearby using a drone or other mobile device could add a strategic dimension to such an attack.

The main variables that amplify the strategic potential of a UAS terror plot align with the unique benefits that drones provide, such as the weapons system providing closeness and intimacy and enhancing target access, which are outlined in the beginning of this section. The third and final section of this report explores the future threat potential associated with drones in greater detail. It does so by documenting the unique and novel ways in which private citizens from around the world have used drones—and in doing so, have further demonstrated what lies within the realm of possibility for terrorists' use of drones in the near future.

290 "Willis, McGill et al., and other terrorism risk researchers operationalize terrorism risk as the product of threat, vulnerability, and consequences. More specifically, threat is usually defined as the probability of an attack (weapon, delivery mode, target, etc.), vulnerability as the probability of an attack's success given that it occurs, and consequences are the losses that occur (fatalities, injuries, direct and indirect economic impacts, among others) given a successful attack." Barry Charles Ezell et al., "Probalistic Risk Analysis and Terrorism Risk," *Risk Analysis* 30:4 (2010): p. 577; for additional background, see Henry H. Willis et al., *Estimating Terrorism Risk* (Santa Monica, CA: RAND Corporation, 2005); and John A. Major, "Advanced Techniques for Modeling Terrorism Risk," *Journal of Risk Finance*, Fall 2012, pp. 15–24. The author defines a low-consequence event as one that results in any of the following: no casualties or a very limited loss of life (a few deaths); minor physical damage or economic impact; or none or a small, limited psychological impact. A moderate-consequence event would be one that resulted in more than a few to a hundred deaths, significant structural damage, and a broader psychological impact.

291 I thank Paul Scharre for making this point clear to me.

Section II: Creativity and Complications: The Dark Side of UAS Use and Emerging Technologies

The accessibility of commercial drones has led to an explosion in use of the devices by private citizens. It has also contributed to the fairly rapid development of new ways to use UASs, from fighting forest fires and assisting search-and-rescue missions to delivering packages and racing for sport. There is an obvious benefit to society from these developments, as in many ways UASs can be used to gain efficiencies and to contribute to the public good. Indeed, as noted by Paul Scharre, "uninhabited systems can not only save human lives by undertaking dangerous missions in their place, they can enable new concepts of operation that would not be possible were human lives at risk."[292]

While private-sector drone makers and software developers are providing the tools to enable UAS exploration, the decentralization of UAS technology has created a playing field in which individual users are limited only by their own imaginations and the various government regulations to which they choose to abide—if the regulations even exist. In this way, when it comes to innovation in UAS use, creativity is king. A number of emerging technologies like autonomy, miniaturization and swarms, and further advancements and increased accessibility of sensors (e.g., forward looking infrared, known by the acronym FLIR) and software (e.g., terrain mapping) will only perpetuate these UAS use trends and extend the realm of the possible.

The dark side to all of this is that innocuous UAS use demonstrated by one person could be exploited by those with more sinister motives. To that end, and to demonstrate more fully what already lies within the realm of the possible for a terrorist group, this section catalogs a number of creative ways that drones have been used by private individuals who did not have terror intent, but whose UAS use could be mimicked or repurposed by others to inflict harm. By focusing on what private citizens have already achieved, we avoid the pitfalls associated with unconstrained brainstorming and "what-if" scenario development about how drones can be used, and limit our discussion to those incidents to which "proof of practicality" applies.[293] The section concludes with a brief review of emerging technology trends, and discusses how they will complicate future terrorists' use of drones, and the threat potential as a delivery or attack mechanism they hold.

Creativity and Additional Capability

> *For example, the first thing many people often ask is: "What weapon should I use in my operation?" But the answer to this question—and it's an important question—is not as difficult as it may seem. The Mujahid Brother Nidal Hasan used firearms in his assault on Fort Hood, but the fact is, today's Mujahid is no longer limited to bullets and bombs when it comes to his choice of a weapon. As the blessed operations of September 11th showed, a little imagination and planning and a minimal budget can turn almost anything into a deadly, effective and convenient weapon which can take the enemy by surprise and deprive him of sleep for years on end.*
>
> *—Adam Gadahn, 2010*[294]

As the 2010 quote from the late al-Qa`ida operative Adam Gadahn makes clear, sometimes all that is required to shock the system in a terrorist campaign is just a little imagination. Thus, to round out our analysis about the current and future threat potential of drones, this subsection focuses not on what

292 Paul Scharre, *Robotics on the Battlefield, Part 1: Range, Persistence and Daring*, (Washington, D.C.: Center for a New American Security, May 2014), p. 27.

293 I would like to thank Brian Jackson for his helpful thoughts, and suggested language, as to how best to frame this section, especially for the "proof of practicality" language that he recommended.

294 Adam Gadahn, "A Call to Arms," *al-Sahab*, January 2010.

terrorists have done, but on what private citizens have. All that would be required from the terrorist side is a little imagination; for that reason, it is equally important that the West's response to the UAS threat be proactive and imaginative as well.

Surveillance

The principal way drones have been used by terrorist groups to date has been for surveillance and strategic communications purposes. Commercially available drones have also been used by private citizens for a range of snooping purposes, including spying on backyard neighbors or stealing trade secrets via industrial-corporate espionage.[295] UAS flights have also been observed over strategic military installations in the United States, such as those that have taken place over Naval Base Klitsap.[296]

Given the array of sensors and other add-ons that are available, the surveillance potential of today's commercially available drones is not limited to aerial intelligence or line-of-sight reconnaissance. The actions taken by two security consultants at the Black Hat security conference in 2011 demonstrate what can be accomplished with a little know-how and ingenuity. Armed with several thousand dollars and using "off-the-shelf electronics" the two experts created (in their garage) the Wireless Aerial Surveillance Platform, or WASP, a UAS with unique capabilities.[297] As noted by *Forbes*:

> The WASP, built from a retired Army target drone converted from a gasoline engine to electric batteries, is equipped with an HD camera, a cigarette-pack sized on-board Linux computer packed with network-hacking tools including the BackTrack testing toolset and a custom-built 340 million word dictionary for brute-force guessing of passwords, and eleven antennae…
>
> On top of cracking wifi networks, the upgraded WASP now also performs a new trick: impersonating the GSM cell phone towers used by AT&T and T-Mobile to trick phones into connecting to the plane's antenna rather than their carrier, allowing the drone to record conversations and text messages on 32 gigabytes of storage. A 4G T-mobile card routes the communications through voice-over-Internet or traditional phone connections to avoid dropping the call.[298]

That was nearly five years ago, and while security services are aware of these vulnerabilities, the ability to mimic and re-create the WASP system exists. As noted by Jane's:

> Fully functional drone systems that require no assembly are already available for purchase by the general public. The AR Parrot Drone, for example, costs USD300, is controlled using a smartphone and sends back real-time video feed to the operator's smartphone or tablet computer. When modified with a lightweight computer running Linux, a broadband connection, a GPS receiver and two WiFi cards, the Parrot can be turned into a drone that is capable of hacking into WiFi systems and carrying out rudimentary signals intelligence.[299]

Accessing Sensitive Locations and VIPs

The potential of violent actors to access sensitive sites has been demonstrated by a number of cases that involve private citizens who were able to fly drones into or over a number of hard-to-access, restricted locations. One of the most famous examples occurred in January 2015 when an off-duty U.S. government employee "lost control of a friend's DJI Phantom quadcopter, which then crashed onto

295 For corporate security linkages, see "New Threat: Drones Banned for Fear of Espionage," *White Sparks* 7:145 (March 10, 2015); see also Michael Condon, "Feedlots Concerned about Industrial Espionage from Drones," ABC Rural, April 2, 2013.

296 "Navy Looking for Drone Operator Flying Device around Washington State Base," Fox News, February 27, 2016.

297 Pierluigi Paganini, "Wireless Aerial Surveillance Platform, the DIY Spy Drone," Security Affairs, December 17, 2014.

298 Andy Greenberg, "Flying Drone Can Crack Wi-Fi Networks, Snoop on Cellphones," *Forbes*, July 28, 2011.

299 "Attack of the Drones—the Dangers of Remote-Controlled Aircraft," *Jane's Intelligence Review*, December 16, 2011.

the White House lawn." The individual who was flying the UAS was intoxicated at the time and is believed to have flown the UAS onto the White House grounds by accident. The trouble for the Secret Service was that the incident appears to have motivated someone else to try to pull off the same stunt intentionally in May of that same year. In this incident, "a man was arrested for trying to fly a Parrot Bebop drone over the White House fence."[300] UAS flights over sensitive locations by private citizens have also been an issue in France, as "unidentified drones have been flown over the US embassy, the Eiffel Tower, the Invalides military museum, the submarine communications base at Sainte-Assise, the Place de la Concorde, the Elysee Palace and multiple nuclear power stations."[301] As noted in section I, Maynard Hill also made headlines in 2003 for flying a UAS across the Atlantic Ocean on less than a gallon of gas.[302]

Photo Credit: Screen grab of Pirate Party UAS at Angela Merkel press event

Commercially available drones also have the potential to provide greater access to political leaders and other VIPs. For example, in September 2013 activists from the German Pirate Party made news after they successfully flew "a small Parrot quadcopter drone up to the stage" where German chancellor Angela Merkel was speaking to a rally of supporters.[303] The activist controlling the UAS was able to hover the UAS over her head and in front of her before he was arrested.[304] "Commentators noted that if the drone been equipped with even a small explosive device, it could have been an effective weapon."[305]

The boldest and perhaps most troublesome incident to date occurred in August 2015, when a Japanese activist, protesting Japan's nuclear policy, successfully flew and landed a UAS "carrying trace amounts of radiation" onto the roof of the Japanese prime minister's residence.[306] While the activist conducted the stunt for publicity and not to inflict harm on the prime minister, the incident still speaks to what lies within the same realm of possibility for a group that has violent intentions.

Drones have also been used to smuggle drugs across borders, to deliver material into entry-control-restricted locations, such as prisons, and to conduct corporate espionage. According to estimates provided by the U.S. Drug Enforcement Agency (DEA), in 2014 there were "in excess of 150 cross-border smuggling flights" involving drones that flew across either the U.S.-Mexico or U.S.-Canada borders.[307] While the DEA and other agencies have been aware of this issue, U.S. officials seized their first ship-

300 Abbott et al., "Hostile Drones.

301 Ibid.

302 Sohn, "Model Airplane Flies the Atlantic."

303 Timothy B. Lee, "Watch the Pirate Party Fly a Drone in Front of Germany's Chancellor," *Washington Post*, September 18, 2013; Dan Gettinger, "A Pirate Drone in Germany," Center for the Study of the Drone, September 19, 2013.

304 Lee, "Watch the Pirate Party Fly a Drone in Front of Germany's Chancellor."

305 Gettinger et al., *The Drone Primer*, p. 9.

306 Scott Mitchell, "Someone Flew a Drone Carrying Radioactive Material on to the Japanese PM's Office," Vice, April 22, 2015.

307 Friese et al., "Emerging Unmanned Threats," p. 47; for additional background, see Kristina Davis, "Two plead guilty in border drug smuggling by drone," *Los Angeles Times*, August 12, 2015.

ment of drugs delivered via cross-border drone only in August 2015.[308] Prison officials in numerous countries have faced similar challenges. For example, in 2012 "a $600 remote-controlled quadcopter [was flown] over a Brazilian prison fence to deliver cell phones to the incarcerated."[309] Drones have also been used to deliver contraband, pornography, weapons and food to inmates, and by kidnappers to pick up a ransom payment.[310] Although their platforms have not been that capable, a number of DIY hobbyists have used UAS technology to build systems large enough and with a sufficient amount of lift to transport a person.[311] These examples speak to the broader utility of drones for terrorist organizations, and illustrate how—just like Amazon's plan to use drones to deliver packages—terrorists might be eyeing drone platforms to deliver sensitive matériel or to function as couriers.

Weaponize

As outlined in the typology presented in section I, there are several ways to weaponize a UAS. They include piloting a UAS to a target; using a UAS to deliver an explosive or to disperse chemical, biological or radiological material; and mounting a weapon to a UAS. Like the examples earlier in this subsection, a variety of incidents involving private citizens demonstrate what is already in the realm of possibility when it comes to using commercially available drones in a violent, weaponized way.

Pilot to Target

Akin to Japan's use of kamikaze pilots during World War II, a terrorist can pilot a UAS directly to his or her target. There are two main threat angles associated with this type of attack. The first involves the piloting of an explosive-laden UAS into an intended target. Some have dubbed this type of approach, which Iran has declared its intent to use, the "kamikaze or suicide drone."[312] The second attack method involves the piloting of a UAS into a target that could have catastrophic consequences if hit in the right location, such as a large commercial airliner's engine (i.e., a "birdstrike" scenario), precluding the need for explosives.[313] In this type of attack, the UAS itself functions as the weapon, and the "explosive" lies in the creative and sinister way in which the drone is used. Naturally, both of these attack methods can be used in combination with one another, and in the future the threat potential of this approach will be complicated by UAS swarms (for further detail, see later in this paper), whereby a commercial airliner or other target needs to avoid not one UAS but many, with the potential to overwhelm a particular system. For example, UAS controllers could position themselves along the final route of approach used by lower- and slower-flying incoming aircraft at Newark Liberty International Airport. The danger potentially caused by a last-minute landing problem at Newark could be amplified, considering that one of the airport's runways runs adjacent to a major (and heavily trafficked) highway.

AeroVironment's small, backpack-portable Switchblade UAS, which the U.S. military is in the process of fielding, illustrates the potential of "kamikaze" UAS systems.[314] The device also provides a glimpse into how small "kamikaze"-style UASs are bound to significantly alter the tactics, techniques and procedures of conventional militaries, insurgents and terrorists alike. The value of the Switchblade lies in its transportability, weight and destructive potential. As noted by *Gizmodo*, the device:

> Carries a small explosive charge equivalent to a 40mm grenade, allowing it to target lightly ar-

308 Ibid.

309 Marc Goodman, "Criminals and Terrorists Can Use Drones Too," *Time*, January 31, 2013.

310 Mary Emily O'Hara, "Another Drone was Used to Smuggle Contraband into a Prison," Vice, August 1, 2014; Kevin Poulson, "Drones and Spyware: The Bizarre Tale of a Brutal Kidnapping," *Wired*, July 24, 2015.

311 For example, see "Self flying drone is powerful enough to carry a person," *Daily Mail* (Video), no date.

312 "Iran Helping Hamas, Hezbollah Build Fleet of Suicide Drones," *Jerusalem Post*, April 9, 2015.

313 For background on this issue, see Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles*, pp. 26–28.

314 Even more lightweight than the Switchblade, Prioria's Maveric UAS also illustrates this potential.

> mored vehicles and embedded (or otherwise inaccessible) infantry positions, such as on rooftops or ridge lines. What's more, the Switchblade's electric propulsion system and small stature make is a sneaky little bastard, difficult to track and able to glide silently in a window before detonating.[315]

The U.S. military is also using even smaller, hand-launched drones like the Wasp or Raven to enhance the field surveillance capabilities of operational units. The size and cost of these UAS allows them to be purchased in the thousands, and as technology advances, future drones will get even smaller.

These drones are beyond the accessibility of terrorist groups, but that does not mean that creative terror actors will not seek to replicate the Switchblade's key features, even if done in an ad hoc or jerry-built way. For example, as noted by *Newsweek*, "*Wired* magazine editor Chris Anderson built a version of the military's hand-tossed Raven surveillance drone for $1,000, while an Arizona-based anti-immigrant group instituted its own pilotless surveillance system to monitor the U.S.-Mexico border for just $25,000."[316] Another potential way to create a "kamikaze" UAS on the cheap would be for a terrorist group to cobble together existing resources, such as outfitting a small fixed-wing aircraft like a Cessna with autopilot or GPS guidance and remote-control features, and then loading that heavier-payload-capable craft with explosives. When drones were in short supply in the first decade of the twenty-first century, this approach was something the U.S. military considered as a cheap, stopgap measure to get more reconnaissance and armed drones into the sky.[317]

As has been well reported, a steady stream of close encounters between private drones and commercial airliners has taken place in flight over the last several years. To gain analytical purchase into this issue, the Center for the Study of the Drone at Bard College released a report in 2015 that analyzed 921 incidents in the United States over a nearly two-year period during which a UAS either was sighted by "a pilot or an air traffic controller… [who observed the UAS] flying within or near the flight paths of manned aircraft" or when a UAS came in close enough proximity to a manned aircraft that the potential for a "near midair collision" existed.[318] In their report, Dan Gettinger and Arthur Holland Michel found that 35.5 percent of the 921 incidents were close enough to be deemed "close encounters."[319] Further, the authors

> counted 158 incidents in which a drone came within 200 feet or less of a manned aircraft (two-thirds of all Close Encounters in which a concrete drone-to-aircraft proximity is given), 51 incidents in which the proximity was 50 feet or less, and 28 incidents in which a pilot maneuvered to avoid a collision with a drone. One hundred and sixteen of the Close Encounters involved multiengine jet aircraft, 90 of which were commercial aircraft (the majority of which have the capacity to carry 50 or more passengers). We also counted 38 Close Encounter incidents involving helicopters. The reports do not always clearly identify the type of drone involved in incidents, but of the 340 drones that were identified in the reports, 246 were multirotors (i.e. quadcopters, hexacopters, etc.) and 76 were fixed-wing. The locations with the highest number of incidents were large metropolitan areas.[320]

---

315 Andrew Tarantola, "America's Kamikaze Drone Makes the Skies Way Less Friendly," Gizmodo, September 5, 2013; see also Sam Biddle, "These Drones Transform into Suicide Bombs," Gizmodo, September 9, 2011.

316 Newsweek Staff, "Will Foreign Drones One Day Attack the U.S.?," *Newsweek*, February 25, 2010.

317 Dave Moniz, "Old Planes Eyed as Drones," *USA Today*, February 4, 2002; for additional background, see Gormley, "UAVs and Cruise Missiles as Possible Terrorist Weapons," p. 7; and Dennis Gormley, "Unmanned Air Vehicles as Terror Weapons: Real or Imagined?" NTI, July 1, 2005.

318 Dan Gettinger and Arthur Holland Michel, *Drone Sightings and Close Encounters: An Analysis*, (New York: Center for the Study of the Drone, December 11, 2015), http://dronecenter.bard.edu/drone-sightings-and-close-encounters/.

319 Ibid.

320 Ibid. For additional background, see Craig Whitlock, "Near-Collisions between Drones, Airliners Surge, New FAA Reports Show," *Washington Post*, November 26, 2014; Jonathan Vanian, "Close Calls between Drones and Airliners Are Sky-High," *Forbes*, December 11, 2015.

The frequency of these "close encounters," and specifically the near-miss incidents, has concerned the Federal Aviation Administration. The potential for a UAS to make direct contact with a jet engine or other critical system on a sizable commercial aircraft loaded with passengers while on final approach to an airport and potentially over a densely populated urban area is real. The likelihood of such an event, however, is a matter of debate.[321]

The problem, which Gettinger and Michel also note, is that, with a few exceptions, such as the work being done through the CRASH Lab at Virginia Tech, little testing has been done.[322] There is a paucity of empirical, physical test-driven data to evaluate just how much risk exists.[323] The computer simulations run by Virginia Tech's lab suggest that, depending on the strike location and the size of the UAS, a UAS collision with an airliner has the potential to cause "critical damage."[324]

A factor that complicates this issue slightly is an open-source "zombie drone" software-hardware package that allows one to hack into, "hijack" and then take control of a nearby commercially available UAS. This approach would allow violently motivated actors to potentially repurpose UAS already in flight.[325] Although a matter of dispute, Iran claims that in 2011 it was able to hack into and take over the controls of an RQ-170 Sentinel, a super-stealthy and advanced military-grade U.S. UAS, which, if true, would illustrate that there is precedent for this type of action on a much larger scale.[326]

Deliver or Drop Explosive

While a UAS loaded with explosives can be piloted directly to its objective, a UAS can also be modified to drop an explosive over a target, such as a VIP gathering or a stadium full of people. UAS hobbyists looking for a thrill, a good aerial shot or to make the news have already flown drones over stadiums. Indeed, drones have been spotted over college and NFL football games, professional soccer matches in a number of countries and the U.S. Open. During that latter event, which occurred after the U.S. Federal Aviation Administration prohibited UAS flights over stadiums in the fall of 2014, a UAS "whizzed above players Flavia Pennetta and Monica Niculescu before slamming into an empty area at Louis Armstrong Stadium."[327]

Facilitating the delivery or the dropping of an explosive is commercial off-the-shelf technology designed to initiate the release of a payload, which already exists. The availability of such tools suggests that the "jump" for terrorists employing this type of tactic is not far away. As noted by the defense consultancy Jane's in late 2011:

---

321 According to Fred Roggero, the "potential for catastrophic damage is certainly there." His perspective carries some weight, as he is "a retired Air Force major general who was in charge of aviation safety investigations for the service and now serves as a consultant to companies seeking to fly drones commercially." For background, see Whitlock, "Near-Collisions between Drones, Airliners Surge." While a number of experts agree with Roggero or have similar views, other specialists believe the threat potential is much less and that the risk associated with a UAS–commercial airliner collision is overblown. "We've been flying into birds for how long?" noted John Goglia, a former National Transportation Safety Board member. In his view, a drone isn't "going to bring an airplane down. . . . That's a little bit of baloney." See "Former NTSB Official Says Drone Isn't Going to Bring Airplane Down," *New York Post*, May 8, 2016.

322 Gettinger and Michel, *Drone Sightings and Close Encounters: An Analysis*.

323 Ibid.

324 Ibid.

325 For background, see http://samy.pl/skyjack/.

326 Scott Peterson, "Exclusive: Iran Hijacked US Drone, Says Iranian Engineer," *Christian Science Monitor*, December 15, 2011.

327 Julia Talanova, "Drones Crashing Big Sporting Events, Including U.S. Open, College Football," CNN, September 6, 2015. Russian separatist forces operating in Ukraine in 2014 reportedly outfitted a commercial UAS with a homemade "grenade dropping" mechanism, which they tried to use—unsuccessfully—to attack Ukrainian soldiers from the air. According to the Ukrainian soldiers involved in the incident, the separatists were able to release the grenade over their position, but the grenade failed to detonate for reasons that are unclear. While investigating this issue further, Larry Friese also found a "photograph uploaded to a social media platform [that] shows an improvised assembly configured to drop an RGO or RGN type hand grenade, potentially with additional fragmentation material, from a small UAV." For background see, Friese et al., "Emerging Unmanned Threats," p. 38–39.

> For only USD16.95 anyone can buy the Chinese-made Quanum "bomb" drop system for remote control aircraft. This 23.5 cm long case splits open to release a 103 g payload of the user's choice. It can be installed in just seconds by connecting the bomb with a radio channel so that it can be released on demand. Although sold as a leisure accessory, when used with a drone equipped with GPS navigation and video feed, this type of device could effectively and accurately deliver a pernicious payload on any desired target. The Quanum bomb system, and the many more like it that will surely follow, make it far easier for any terrorist to turn a remote-controlled plane into an aerial bomber.[328]

While attractive to potential terrorist actors, using a UAS in this capacity is not without its own limitations. First, a 103-gram payload, which is roughly equivalent to a quarter of a pound, is not a sizable amount of explosives. Second, as noted by RAND, "conventional bombs are much more effective when employed indoors. An open-air nail-bomb delivered to a crowded outdoor event would, if all went as planned, probably produce effects similar to the Boston marathon attacks."[329] This isn't to say that such an attack should be written off—it shouldn't—but rather that the scale of devastation caused by such an incident might not be higher than that produced by a single suicide bomber. The use of multiple drones or a fleet of autonomous drones could enhance the level of destruction, though.

Weapon Mount

Another attack modality that will likely be explored by terror groups is mounting a weapon directly to a UAS. This wouldn't be that surprising, as some private citizens have been interested in doing the same for quite some time. For example, in December 2008, Jim Simmons, a DIY UAS hobbyist, successfully attached and remotely fired "a Springfield 1911-A .45 caliber weapon with a digital camera gun sight for accurate shooting" to a "Bergen Gasser EB mini-helicopter."[330] The event, a potential first, wasn't just bluster, because Simmons filmed his stunt and posted it online.[331] Few major news outlets reported it, though.

328 "Attack of the Drones."

329 Davis et al., "Armed and Dangerous.

330 As cited ibid. Originally reported by Gizmodo; see Jesus Diaz, "RC Helicopter Modded 45 Caliber Handgun will Probably End in Disaster," Gizmodo, December 10, 2008.

331 For video of the RC helicopter in flight, see www.liveleak.com/view?i=4cd_1228911752.

Photo Credit: Screen grab of Jim Simmons's 2008 Live Leak video

Six and a half years later, in July 2015, a Connecticut teenager, Austin Haughwout, made major new headlines after he posted a video to YouTube that showed him mimicking the stunt, and successfully firing a handgun that he mounted to a commercial UAS variant that he had modified.[332] The video shows the teen remotely firing the handgun while the UAS is in flight through a trigger mechanism he installed.[333] While the teen's accomplishment was certainly novel and noteworthy, the video also shows the jerry-rigged "handgun UAS" bouncing in the air between shots as a result of gun's kickback, indicating that stability and accuracy were central problems affecting the usability and reliability of the platform.[334] (Simmons's device also appears to have faced this problem.) Since the contraption was made by a teenager in the United States, it is almost certain that a terror organization with more resources and expertise would at least be able to mimic the effort, if not improve on it, for potential use in assassination-type scenarios.

Photo Credit: Screen grab of "Flying Gun" YouTube video posted by user Hogwit in 2015

Then, less than six months after his initial media splash, Haughwout made headlines again with another DIY UAS invention. This time he upped the ante and the shock value by creating a UAS-mount-

332 Dan Corcoran and Bob Connors, "Father Says 'Flying Gun' Drone Broke No Laws," NBC Connecticut, July 22, 2015.

333 Ibid.

334 Ibid.

ed flamethrower, which he again successfully demonstrated in another YouTube video posted online.[335] The interesting thing about Haughwout's second invention is that by using a flamethrower instead of a handgun, he was able to improve the weapon's accuracy. In creating this device, Haughwout has not only illustrated the "flamethrower UAS" proof of concept, which he advertised to the world, but he has also shown how easy it is to weaponize a UAS with basic materials.

Photo Credit: Screen grab of "Roasting the Holiday Turkey" YouTube video posted by Hogwit

The actions of Simmons and Haughwout have demonstrated what lies within the realm of possibility in terms of weapon-mounted UAS capability, given a little ingenuity and craftiness.

"Blade" Drone

Although less of a concern, UAS rotator blades also hold a small amount of threat potential due to the high-speeds at which they spin. Accidents involving commercially available drones in 2003, 2005, 2008 and two in 2013, all of which resulted in deaths due to contact made with UAS rotor blades, illustrate the danger.[336] In one unfortunate episode, a UAS flight instructor was struck in the neck by an out-of-control UAS that his student was flying, and the instructor ended up bleeding to death.[337] Another tragic case from 2013 involved an experienced UAS pilot whose head was partially severed after he also lost control of his UAS. Based on what can be learned from news accounts, most if not all of these episodes involved—as one might suspect—larger remote-control helicopters with large and strong blades.[338]

Even smaller drones, however, have caused problems. For example, in November 2015 a UAS blade on a smaller device accidently made contact with a toddler's left eye, and the damage was significant enough to leave the child blind in that eye.[339] To evaluate some of these claims, and the potential for harm, the popular U.S. television show *Mythbusters* conducted an experiment whereby its hosts intentionally flew UAS blades into a chicken carcass to see what would happen, and the damage that would result.[340] The show's hosts were surprised to find that the plastic UAS blades easily sliced into the chicken, leaving them to conclude that if used in close range the blades could inflict some bodily

335 See www.youtube.com/watch?v=lmD3rXUR1Tw.

336 For background on 2003 incident, which resulted in the death of Ronald Kyle, see, www.rcgroups.com/forums/showthread.php?t=165680; for 2005 incident, which reportedly resulted in death of a child in South Korea, see http://rc.runryder.com/helicopter/t169336p1/. Other blade injuries are chronicled at www.heliguy.com/nexus/dangers.html.

337 See www.rcgroups.com/forums/showthread.php?t=165680.

338 Dan Nosowitz, "Remote-Controlled Helicopter Kills 19-Year-Old in Brooklyn," *Popular Science*, September 5, 2013.

339 "Toddler's Eyeball Sliced in Half by Drone Propeller," BBC News, November 26, 2015.

340 Andrew Liptak, "Can a Home Drone Kill You? The Mythbusters Test with a Chicken Says Yes," io9, July 25, 2015.

harm and be dangerous.[341] More damage could probably be done if the blades were metal and the UAS was flown by a skilled operator who could navigate to a target successfully at close range. Even with these modifications, the threat of "blade" drone use still remains low and is more of a potential nuisance than anything else. Given other options, a terrorist actor would likely only select this type of approach to highlight its ability to get close to a VIP or to embarrass a government, rather than inflict a maximum number of casualties.

WMD Delivery

Given their desire for publicity and commitment to violence, a diverse range of terrorist groups have been attracted to the high-lethality potential associated with the use of chemical and biological weapons. The groups that have shown an interest in this type of material range from the Japanese religious cult Aum Shinrikyo to al-Qa`ida to the Covenant, Sword and the Arm of the Lord. Chemical, biological, radiological and nuclear material has been attractive to a number of groups because of the fear and chaos it would inspire and the potential it has to produce many casualties. Yet while a good number of terrorist outfits have experimented with weapons of mass destruction, very few have successfully deployed chemical or biological agents, and most have backed away after experimenting with them. And with one possible exception, none have had success using radiological or nuclear material.[342] Attacks like Aum Shinrikyo's 1994 successful sarin gas attack on the Japanese subway, or the Islamic State's reported use of chemical agents in Syria, are the exception and not the rule. This is because even though WMDs are attractive, acquiring, producing and successfully weaponizing or dispersing these types of agents presents a number of significant technical and logistical hurdles. As noted by RAND:

> The effectiveness of modes for dispersing an attack agent in the air above a target relies on the ability to place sufficient amounts of the weapon in the desired position, its probability of arriving there successfully and at the time designated for the attack, and the chance of successfully dispersing the material in the manner desired.… Particularly for UAVs, the systems' ready availability and ability to fly in most areas that would represent attractive targets appear to be significant advantages. However, they have significant disadvantages in payload size and the probability of successfully deploying the agent at the position and time desired.[343]

Thus, even if they are initially interested, most terror groups soon find out that they do not possess the resources or the level of expertise required to make the investment in WMDs worth it. This is especially the case when they evaluate their WMD options, which add complexity and increases costs (both financial and security, due to the risk associated with being caught trying to acquire or produce this type of material), in relation to the much lower costs of producing and deploying conventional explosives. For most terrorist groups, it doesn't take them long to figure out that the "juice just isn't worth the squeeze" and that it is more effective and efficient to go with more-conventional attack options. For example, instead of using a UAS for the 1993 plot described earlier in this report, Aum Shinrikyo decided to use a spray truck.[344] Given the openness of Western societies, other actors have found it to be more efficient to use the U.S. Postal Service as their delivery mechanism for weaponized anthrax, as the cost of delivery was not more than one or several stamps.[345]

Despite the hurdles terror groups have consistently faced in relation to WMDs, concerns about the

341 Ibid.

342 "To date, the only confirmed case of attempted nuclear terrorism occurred in Russia on November 23, 1995, when Chechen separatists put a crude bomb containing 70 pounds of a mixture of cesium-137 and dynamite in Moscow's Ismailovsky Park. The rebels decided not to detonate this "dirty bomb," but instead informed a national television station to its location." See Graham Allison, "Nuclear Terrorism: How Serious a Threat to Russia," *Russia in Global Affairs*, September–October 2004.

343 Jackson et al., *Evaluating Novel Threats to the Homeland*, p. 25.

344 Danzig et al., "Aum Shinrikyo: Insights into How Terrorists Develop Biological and Chemical Weapons."

345 For background, see "Timeline: How the Anthrax Terror Unfolded," NPR, February 15, 2011.

potential for commercially available drones to be used as platforms to disperse chem-bio material have been around for quite some time. As the cases associated with Aum Shinrikyo and the Islamic State in section I make clear, that concern is not unfounded. During "a 1994 meeting to discuss the future of counter-proliferation in a post-Soviet world, Senator Sam Nunn, the then chairman of the U.S. Senate Committee on Armed Services, laid out three 'out of the box' terrorism scenarios."[346]

> One involved terrorists flying a small UAV loaded with two 40 lb canisters of weaponised Anthrax spores into the Capitol building on the night of the president's State of the Union address to Congress. In Nunn's scenario, terrorists remotely flew the drone from a short distance away and were able to kill hundreds of lawmakers and senior government officials. While the president survived, the government was left paralyzed and a huge, densely populated area was biologically contaminated.[347]

Nearly two decades later, planners in charge of the 2012 summer Olympic Games in London were concerned about a number of aerial threats, including a UAS being used to deliver biological agents. As noted by Brian Fahy, an officer in the UK army, "The range of threats varies in size and capability. It could be a commercial airliner hijacked by somebody with malicious intentions or a protest group using a microlight to get their name in the papers."[348] He added that "it was 'feasible' that remote-controlled aircraft filled with poison and small enough to fit into a backpack could be used as a biological weapon in the capital."[349] The threat was taken seriously enough that the UK armed forces stationed a number of surface-to-air missiles on the tops of high-rise buildings around key Olympic venues.[350] While the surface-to-air missiles likely would not have been used to take down a UAS, a comprehensive plan, which involved other disruption methods, was also developed to ensure people's safety.[351] UK authorities took these precautions based on threat reporting that indicated that the Islamic State was training foreign fighters, including those with links to Britain, to produce toxic material.[352]

The concern about terror use of drones to distribute chem-bio materials has also picked up added steam because UAS platforms are now so much more capable, accessible and affordable. One industry that is now using drones in an analogous way (to disperse chemicals or other pesticides) is the agriculture, as farmers have found drones to be useful for cost savings and to spray wider areas. For example, "a video posted online shows how one Japanese farmer, tired of working in the sweltering heat, turned his remote-controlled helicopter into a crop-duster." As noted by RAND:

> If a terrorist were to use this same concept to spread a lethal agent over a crowd instead of pesticides over rice fields, the potential for harm could be enormous.
>
> One study showed that if 900 g of weapons-grade anthrax was dropped from a height of 100 m upwind of a large US city, an estimated 1.5 million people would become infected, with more than a 100,000 dying. Another study showed the consequences of dispersing a radiological weapon consisting of 2 kg of plutonium and 50 g of cesium over San Diego could lead to an 8 km area being contaminated and thousands of people exposed.[353]

Farmers aren't the only ones who have shown an interest in using drones for dispersion purposes. A

346 "Attack of the Drones."

347 Ibid.

348 Stephanie Condron and Christopher Leake, "Poison Drones Carrying Biological Weapons Are New Olympic Threat, Warns Colonel in Charge of Keeping London Calm," *Daily Mail Online*, May 5, 2012.

349 Ibid.

350 Ibid.

351 Ibid.

352 For background, see Mark Nicol, "MoD Tests Defences against High-Street Drones as MI5 Braces Itself for Jihadi Chemical Attack on UK," *Daily Mail*, September 12, 2015.

353 "Attack of the Drones—the Dangers of Remote-Controlled Aircraft."

graffiti artist in New York City also made news in April 2015 after he successfully attached and used a spraying mechanism to deface a prominently placed billboard of Kendall Jenner in New York City. Both of these cases—of the farmer and graffiti artist—show what one can achieve with a little dedication and ingenuity, and they illustrate that we might not be that far away from someone using a UAS to disperse a chem-bio agent to maim and kill, even if on a small scale.

Complicating Factors

Given the accessibility of commercial drones, the fast pace of technological change and a number of emerging UAS-related technologies, the terrorist UAS threat over the next five to ten years is bound to become more complicated. A cross-cutting challenge, as discussed earlier, is that many of the technological advancements we are seeing and likely will continue to see are being driven not by the military, but by the commercial sector.[354] This means that companies will be motivated and more inclined to open the sale of their technologies to a wider pool of potential buyers. This includes emerging technologies that are going to enhance UAS performance, and add new dimensions to UAS systems. As noted by Paul Scharre:

> Many of the game-changing innovations that enable swarming—low-cost uninhabited systems, autonomy and networking—are driven by commercial sector, not military, innovation. They will be widely available to a range of actors, and many states and non-state groups may be more eager to embrace them than the U.S. military, which is invested heavily in current operational paradigms.[355]

Another complicating issue is that over the course of the next decade, advancements will be made to the hardware and other core factors that currently limit the threat potential of commercially available drones. For example, it is predictable that future off-the-shelf drones will be able to carry heavier payloads, fly and loiter longer, venture farther from their controller, survive in more difficult weather and be able to do so via more-secure communications links (i.e., links that are less prone or susceptible to disruption). Indeed, as noted by Jane's, "the weight of modern onboard navigation equipment and sensors is dropping steadily due to advances in information technology and miniaturization. This allows drone pilots to do more with less."[356] Advancements in power will be a key driver of these developments, and will serve as a barometer of just how quickly UAS payload, range and endurance capabilities change.[357] When compared with advances in software, advances in hardware likely will be more modest.

The speed of small drones, as already illustrated by drone racing variants, and advancements in sensors and UAS add-on technology, such as infrared and night-vision cameras, light detection and ranging (LiDAR) systems and terrain- or facility-mapping tools, will compound these problems, as will things like decentralized manufacturing processes facilitated by 3-D printing, which will make field UAS production and related repairs easier.[358] That does not mean that new commercial UAS variants will be infallible or that the pace of change associated with the various subtechnologies that support drones will be steady, but that even without emerging technology, they will be more capable.

This naturally also means that the tools to counter, disable or defeat UASs will be more capable too. The broader use of commercial drones, as we have already seen, will also be accompanied by regulatory

354 "Joint Doctrine Note 2/11," p. 6–13; Scharre, *Robotics on the Battlefield, Part 2*, p. 42.

355 Scharre, *Robotics on the Battlefield, Part 2*, p. 42.

356 "Attack of the Drones—the Dangers of Remote-Controlled Aircraft."

357 I thank Paul Scharre for this point.

358 For example, see Kit Eaton, "The Perfect Tech Storm: 3-D Printed, Self-Assembling Drone Swarms," *Fast Company*, July 31, 2013; see also Emma Bryce, "This Ultraviolet Printer is 100X Faster than Ordinary 3D Printers," *Wired*, August 13, 2015; and Jordan Golson, "A Military-Grade Drone That Can Be Printed Anywhere," *Wired*, September 16, 2014.

changes that will likely lead to a further rationalization of airspace and export-control restrictions; factors that could make it harder for terrorist actors to acquire specific technology or fly drones when and where they want to.[359] The evolution of defensive tactics will pose challenges for terrorists as well.

Emerging technologies that have disruptive potential complicate things even more. Some of the most significant technologies that will drive changes in UAS capabilities include artificial intelligence, autonomous systems and robotics; miniaturization and swarming; nanoexplosives and directed-energy weapons; enhanced processing power and data mining; and cyber tools.[360] Advancements in autonomy, which are occurring rapidly, are bound to create new opportunities for terrorists and state agents alike, as changes in this area allow for a person or group to simultaneously operate multiple drones and potentially cause more destruction as a result.[361] While each of these technologies will present its own set of counterterrorism challenges, future terrorist threats, specifically those involving drones, likely will be tied to the combined use of several of these technologies as a system.

For example, imagine a scenario in which a terrorist group is able to design and print its own micro-drones by the thousands using a commercially available 3-D printer, a feat that researchers at Harvard University have already accomplished.[362] Powered by new and smaller energy sources, these micro-drones could then be programmed to fly autonomously as part of a large, networked swarm, whereby they would aim to overwhelm "enemy defense by their sheer numbers."[363] A terrorist group could develop several of these UAS swarms, some as general deception (to distract and confuse authorities) and others with larger and more capable UASs loaded with chemical or biological weapons hidden within the UAS swarm clouds. Using software that will enable the discovery of large collections of people (perhaps based on their mass, heat or digital signatures) in an urban environment, these larger drones would hunt down these high-density groups and release their toxic agents via air delivery so they could inflict the most harm. (Researchers affiliated with Central European University have already developed software for UASs that evaluates the size of crowds.[364])

The accompanying microswarms could be programmed to achieve three supporting tasks: (1) to protect the larger drones (i.e., by defeating local UAS countermeasure systems) and to ensure the successful delivery of the toxic agents; (2) to film and broadcast the attack; and (3) to fly through the dispersion area immediately after chem-bio release, and then to other nearby areas so the zone of contamination could be extended.[365] Borrowing a style of attack that is already popular with today's terrorist groups, the attack could be designed as a phased or multipronged operation, just like LeT's

359 I thank Brian Jackson for highlighting this point.

360 For background on these issues, see Ben FitzGerald, Kelley Sayler and Shawn Brimley, "Game Changers: Disruptive Technology and U.S. Defense Strategy," Center for a New American Security, September 27, 2013; see also James Manyika et al., "Disruptive Technologies: Advances That Will Transform Life, Business and the Global Economy," McKinsey Global Institute, May 2013. See also "Joint Doctrine Note 2/11," pp. 62–71; T. X. Hammes, "In an Era of Cheap Drones: US Can't Afford Exquisite Weapons," Defense One, January 16, 2016; T. X. Hammes, "Technologies Converge and Power Diffuses: The Evolution of Small, Smart, and Cheap Weapons," *Policy Analysis* (CATO Institute), no. 786, January 27, 2016. Autonomy "refers to a specific action that a machine can take independently, without human intervention." See Samuel J. Brannen, *Sustaining the U.S. Lead in Unmanned Systems: Military and Homeland Considerations through 2025* (Washington, D.C.: Center for Strategic and International Studies, February 2014), p. 5; for background on robots and robotics see Scharre, Robotics on the Battlefield, Part 2, p. 11.

361 I thank Paul Scharre for his suggestions related to this issue.

362 For background, see Scharre, *Robotics on the Battlefield, Part 2*, p. 20; Radhika Nagpal, "The Kilobot Project," www.eecs.harvard.edu/ssr/projects/progSA/kilobot.html; see also Eaton, "The Perfect Tech Storm;" for other threat-scenario variations involving potential future terrorist use of UASs, see Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles*, pp. 28–33.

363 As noted by Paul Scharre: "The point of building large numbers of lower cost systems is not to field forces on the battlefield that are qualitatively inferior to the enemy. Rather, it is to change the notion of qualitative superiority from an attribute of the platform to an attribute of the swarm. The swarm, as a whole, should be more capable than an adversary's military forces." See Scharre, *Robotics on the Battlefield, Part 2*, p. 10, 21.

364 For background, see Austin Choi-Fitzpatrick's "Drones for Good" project at www.austinchoifitzpatrick.com/dronesforgood/.

365 The Naval Postgraduate School is already experimenting with UAS swarm–fighting scenarios. See "Dogfighting Drones—Swarms of Unmanned Battle-Bots Take to the Skies," airforce-technology.com, July 23, 2012.

devastating November 2008 attack in Mumbai, which involved the terrorists attacking four targets simultaneously.

An attack like this one may never materialize, but the introduction of these new technologies will create additional system-based options for terrorist groups, a trend that will favor the creative and make counterterrorism harder. This is a future that will require agile, outside-the-box thinking, as terrorists, as they always do, will seek to outwit their opponents and level the asymmetric playing field through a mix of cunning and bold operations. Even though the United States and other Western countries are the principal agents developing this technology, it is not clear if they are prepared for this future and what it might mean in the counterterrorism domain, as these technologies are shifting strength from hard power and conventional weapons to the artistic—solutions that involve the combined use of inputs that are small, fast and many. The Islamic State's use and manipulation of Twitter is one good example of this. Indeed, as noted by Paul Scharre, "the history of revolutions in warfare has shown they are won by those who uncover the most effective ways of using new technologies, not necessarily those who invent the technology first or even have the best technology."[366] The immediate danger posed by terrorist use of UAS lies in human-machine teaming, and it is in that area that the world will get a glimpse of the future potential—and complexities—that emerging technologies hold.

366 For background see Scharre, *Robotics on the Battlefield, Part 2*, p. 42.

Conclusion

Those worried about drone proliferation must face facts. We are no longer in a world where only the United States has the technology, and we are not moving toward a future in which the technology is used only in the same way we use it now.

—Peter Singer, 2013[367]

There will be imitators—crude at first—but inevitably better and better, and while reasonable people can disagree on how long it will take before terrorists, insurgents, and other rogue groups can build or acquire weaponized drones that can be guided by video straight into a target, there's really no dispute that it is a question of when and not if. The day will come when such drones are available to almost anyone who wants them badly enough.

—John Villasenor, 2011[368]

As the two quotes that open this section illustrate, the future we want is not always the future that we will be lucky enough to have. Through an analysis of proven terror-linked UAS cases, and a similar review of creative ways that individual citizens have used the technology, this report has sought to provide deep insight into the current UAS terror threat and the future capability that lies right around the corner. By cataloging vetted terror UAS cases and setting them against a timeline and an analytical framework, this report has also aimed to provide foundational data so more-systematic and robust tracking of this phenomenon, and empirically driven investigations into other research questions (e.g., whether UASs in the hands of terrorist actors are or will be transformative), can occur.[369]

Despite claims to the contrary, terrorist usage of and interest in drones is not a new issue, but rather an issue with roots that are now more than two decades old. While the initial terror UAS pioneer was a Japanese apocalyptic group, terrorist interest in drones as an attack platform has been diverse and has spanned a number of ideologies and geographic regions. The primary way terror groups or individuals have used drones to date has been for surveillance and strategic communications purposes. Although much less successfully, a smaller number of terror actors have sought to weaponize drones; the first known attempt involving a flight to do so was conducted by Hezbollah over a decade ago. As one could easily predict, given the lower cost and increased accessibility of commercial UAS platforms, attempts at weaponization have become more frequent since then.

Currently, the use of a single UAS by terrorists piloted by remote control remains a "niche" threat and is best understood as being a moderate probability, and low-to-moderate threat in terms of lethality (several strategic uses, as outlined in section I, notwithstanding). While the use of a group of drones, or an autonomous swarm, by terrorist entities has not yet been observed, the use of more and more sophisticated drones is likely to enhance the scope and seriousness of the threat, and affect the consequence of future incidents.

Terrorist use of drones has also yet to reach a tipping point in terms of its diffusion, but it appears as though that future does not lie that far away, as there a number of drivers that make such a future more likely. First, the broad proliferation of drones, and the simultaneous downsizing of platforms and the enhancing of their capabilities and add-on features, makes them only more attractive and financially and logistically more accessible. Indeed, as Michael Horowitz's adoption-capacity theory of the diffusion of major military innovations predicts, a reduction in the cost per unit of a technology and an

367 Peter Singer, "The Global Swarm," *Foreign Policy*, March 11, 2013.

368 John Villasenor, "Armchair Kamikaze: What the Latest Generation of Small Armed Drones Means for Anti-Terrorism," Brookings, October 6, 2011.

369 For background on the question of whether UAS are transformative or revolutionary, see Davis et al., "Armed and Dangerous," p. 11; Peter Singer, "The Predator Comes Home: A Primer on Domestic Drones, Their Huge Business Opportunities, and Their Deep Political, Moral, and Legal Challenges," Brookings, March 8, 2013.

increase in the commercial applications of that technology is likely to be accompanied by an enhanced rate of adoption.[370] Integrating commercially available drones into their "capability toolkit" also does not require large-scale organizational change for terrorist groups, especially when they are used only for surveillance and strategic communications purposes.[371] This dynamic also strongly suggests that even more terrorist entities will adopt and use the technology in the future.[372]

Second, in the digital environment in which we live, groups may easily learn from one another and spot new ideas generated by others that they can repurpose. In this way, demonstrated instances of creative UAS use by private citizens, which could easily have violent applications, expand the immediate capability profile of drones for a terrorist entity, and have strong potential to fuel copycat or derivative weaponization attempts by those who want to inflict harm. Such a dynamic has the potential to speed up learning and contribute to more creative and rapid fielding of homemade "outside-the-box" attack options.

Third, as noted by Peter Singer, the accessibility and stand-off distance provided by commercial drones "allows new players into the game," especially those less inclined to carry out a suicide operation.[373] Fourth, the prevention of these types of scenarios is only as good as our ability to think in similar, creative ways, and as good as the technology and countermeasures that are developed to disrupt or disable UAS before they reach their objective. Those tasks may sound simple, but knowing where to deploy defensive systems or having the capability to rapidly deploy them to other locales is a task not without its own share of challenges.

Four interrelated implications from this research can help us better prepare for the future. First, if not already being done on a broad scale, the U.S. government should start systematically cataloging cases of proven UAS interest and use by terrorist actors, as well as innovative ways that private citizens have used the devices. This data should then be situated against a framework, similar to the one presented earlier in this report, that will allow those tracking this threat to quickly identify noteworthy developments and better understand the evolution of this phenomenon. Such a resource could initially be created and maintained with minimal resources and effort, and it would pay dividends in the years ahead as it would help government officials make more informed resourcing and regulatory decisions, which in turn should promote more effective UAS policies.

A second related implication pertains to the analysis of UAS cases. As argued in this report, the nature of the terrorist UAS threat isn't an issue that can fully be understood by looking at developments in the terrorism sphere alone. Indeed, evaluating the terrorist UAS threat is just as much about paying attention to related innovative developments that occur in private industry, academia and by creatively minded hobbyists, as it is about monitoring terrorist actors and their activity. To stay current and to limit the risk of strategic surprise, intelligence analysts following this issue need to monitor innovations across a number of spheres, and be part terror specialist, part technologist, and part industry expert. They need to be schooled in the monitoring and collection of open-source material, as the overwhelming majority of game-changing developments in this sphere are taking place in plain sight.

A third issue is the applicability of this research to similar problems, such as the use of robotics and remote-control and autonomous technology by terrorists to conduct future attacks using ground and maritime drone vehicles.[374] Insurgents in Iraq have been working since at least 2011 to integrate re-

370 Michael Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (New Jersey: Princeton University Press, 2010), pp. 9–11.

371 Ibid.

372 It can be argued that modifying commercially available UASs so they become weaponized could require more organizational capacity, and thus limit the diffusion of UAS being used by terrorists in that way.

373 Singer, "The Predator Comes Home."

374 I would like to thank Paul Scharre for his recommendation to include this topic.

mote-control features into full-size vehicles so they could be loaded with explosives, navigated to their target and detonated from a safe stand-off distance.[375] Over the last three years, at least four different Syrian insurgent factions have deployed remote-control vehicle-borne improvised explosive devices.[376] Available evidence suggests that all of these cases involved human-machine teaming. Footage obtained by Sky News also illustrates that the Islamic State is experimenting with, and seeking to field, the same type of technology.[377] A predictable evolution of this approach would be for terrorist groups, and potentially individuals motivated by them in the West, to obtain "self-driving" vehicles, which already have autonomous features and are able to self-navigate, and load them with conventional explosives. Not having to use a driver would mean that those planning the attack could, at least in theory, continue to conduct additional attacks using multiple cars until they were caught.

Last, the government should remain open minded and equally creative about the structures it creates, both inside and out government, to facilitate the meaningful exchange of ideas and who it brings into its tent to serve as advisers. This would include creating or developing teams with a diversity of perspectives and skills, potentially networked via a joint interagency task force or working group, to investigate and track the threat, and to propose low-cost solutions to counter future UAS terror activity. As evidenced by investments the U.S. government has made in the development of UAS countermeasures, and the teams that are supporting those endeavors, the government has already been inclusively minded in this regard. Yet it still remains an open question as to whether those efforts, on both the red-teaming and countermeasure sides, go far enough or are forward-leaning enough. Serious attempts to game out future terror UAS use must be informed by those who produce the technology, those who write and comment on the technology and its disruption potential, those who study terrorism, hobbyists who have pioneered innovative ways to use UASs and those—like drone racers—who are pushing the limits of UAS technology.

375 Noah Schatman, "Iraq Militants Brag: We've Got Robotic Weapons, Too," *Wired*, April 10, 2011.

376 For examples, see Ben Makuch, "The Frontline of DIY Weaponry is in Syria," Motherboard, May 24, 2014; www.youtube.com/watch?v=T5NFfsemURo; www.youtube.com/watch?v=JkY1rQyIiOU; www.youtube.com/watch?v=944JXHXnLIQ; www.youtube.com/watch?v=fyn5jxQZh5A; www.youtube.com/watch?v=_3dGVxpwHHc; www.youtube.com/watch?v=MFFYoD56kek.

377 Stuart Ramsey, "Exclusive: Inside IS Terror Weapons Lab," Sky News, July 4, 2016.

Appendices

I: Other UAS Classification Schemes

Class	Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Civil Category (UK CAA)	Example Platform
Class I <150 kg	MICRO < 2 kg	Tactical Platoon, Section, Individual (single operator)	Up to 200ft AGL	5 km (Line of Sight (LOS))	Weight Classification Group (WCG) 1 Small Unmanned Aircraft (<20 kg)	Black Widow
	MINI 2-20[13] kg	Tactical Sub-Unit (manual launch)	Up to 3000ft AGL	25 km (LOS)		Scan Eagle, Skylark, Raven, DH3
	SMALL > 20 kg	Tactical Unit (employs launch system)	Up to 5000ft AGL	50 km (LOS)	WCG 2 Light Unmanned Aircraft (20><150 kg)	Luna, Hermes 90
Class II 150–600kg	TACTICAL	Tactical Formation	Up to 10,000ft AGL	200 km (LOS)	WCG 3 UAV (>150 kg)	Sperwer, Iview 250, Aerostar, Watchkeeper
Class III >600 kg	Medium Altitude, Long Endurance (MALE)[14]	Operational/ Theatre	Up to 45,000ft AGL	Unlimited (BLOS)		Reaper, Heron, Hermes 900
	High Altitude, Long Endurance (HALE)	Strategic/ National	Up to 65,000ft AGL	Unlimited (BLOS)		Global Hawk
	Strike/ Combat	Strategic/ National	Up to 65,000ft AGL	Unlimited (BLOS)		

Source: "Joint Doctrine Note 2/11: The UK Approach to Unmanned Aircraft Systems," p. 2-7.

Category	Mini	Tactical	Strategic
Altitude	Low	Low to medium	Medium to high
Endurance	Short (about an hour)	Medium (up to several hours)	Long (ranges from hours to days)
Range	Close-range	Limited to line-of-sight (approximately 300 kilometers or less) (about 186 miles)	Long range
Example	Raven 	Shadow 	Global Hawk 

Source: "Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports," GAO Report 12-536, July 2012, p. 4.

II: Select List of Commercial UASs and their Capabilities

Table 1. Select list of commercially available UAVs

Model	Weight	Payload	Flight time	Range	Max speed	Camera	Operating conditions	Price
Parrot BeeBop	0.4 kg	0 kg	12 mins	250 m (extendable)	29 mph	Yes (14MP)	Dry conditions only	£700-900 (RTF)
Blade 350 QX2	1 kg	0.2 kg	10 mins	1,000 m	32 mph	Yes	Dry conditions only	£200-300 (RTF)
3DR IRIS+	0.9 kg	0.2 kg	16 mins	800-1,000 m	40 mph	Yes	Dry conditions only	£500-600 (RTF)
DJI Phantom 2 Vision +	1.2 kg	0.2 kg	25 mins	600 m	33 mph	Yes (14MP)	Dry conditions only	£800-1,200
DJI Phantom 3 Professional	1.2 kg	0.3 kg	28 mins	1,900 m	35 mph	Yes (12MP)	Dry conditions only	£1,000-1,200
Walkera Scout X4	1.7 kg	0.5-1.0 kg	25 mins	1,200 m	40-50 mph	Yes	Dry conditions only	£700-900
Yuneec Q500 Typhoon	1.1 kg	0.5 kg	25 mins	600 m	54 mph	Yes (12MP)	Dry conditions only	£900-1,100 (RTF)
SkyJib-X4 XL Ti-QR	15 kg	7.5 kg	15 mins	3,000-25,000 m	24 mph	Yes	Wind	£7,500-8,000
Altura Zenith ATX8	3.1 kg	2.9 kg	45 mins	1,000 m	44 mph	Yes	Light rain/ snow	£15,000-20,000
MicroDrones MD4-1000	2.65 kg	1.2 kg	88 mins	5,000 m	26 mph	Yes	Light rain/ snow	£20,000-30,000

Source: Chris Abbott et al., "Hostile Drones: the Hostile Use of Drones against British Targets," Remote Control Project, January 2016, p. 5.[378]

378 For an overview of UAS-related sensors and their capabilities, see Friese et al., "Emerging Unmanned Threats," pp. 24–25.